MATERIAL EXLUVISO
GRUPO CURSO FÁCIL
CLIQUE AQUI
E ACESSE + MATERIAIS
Curso Fácil

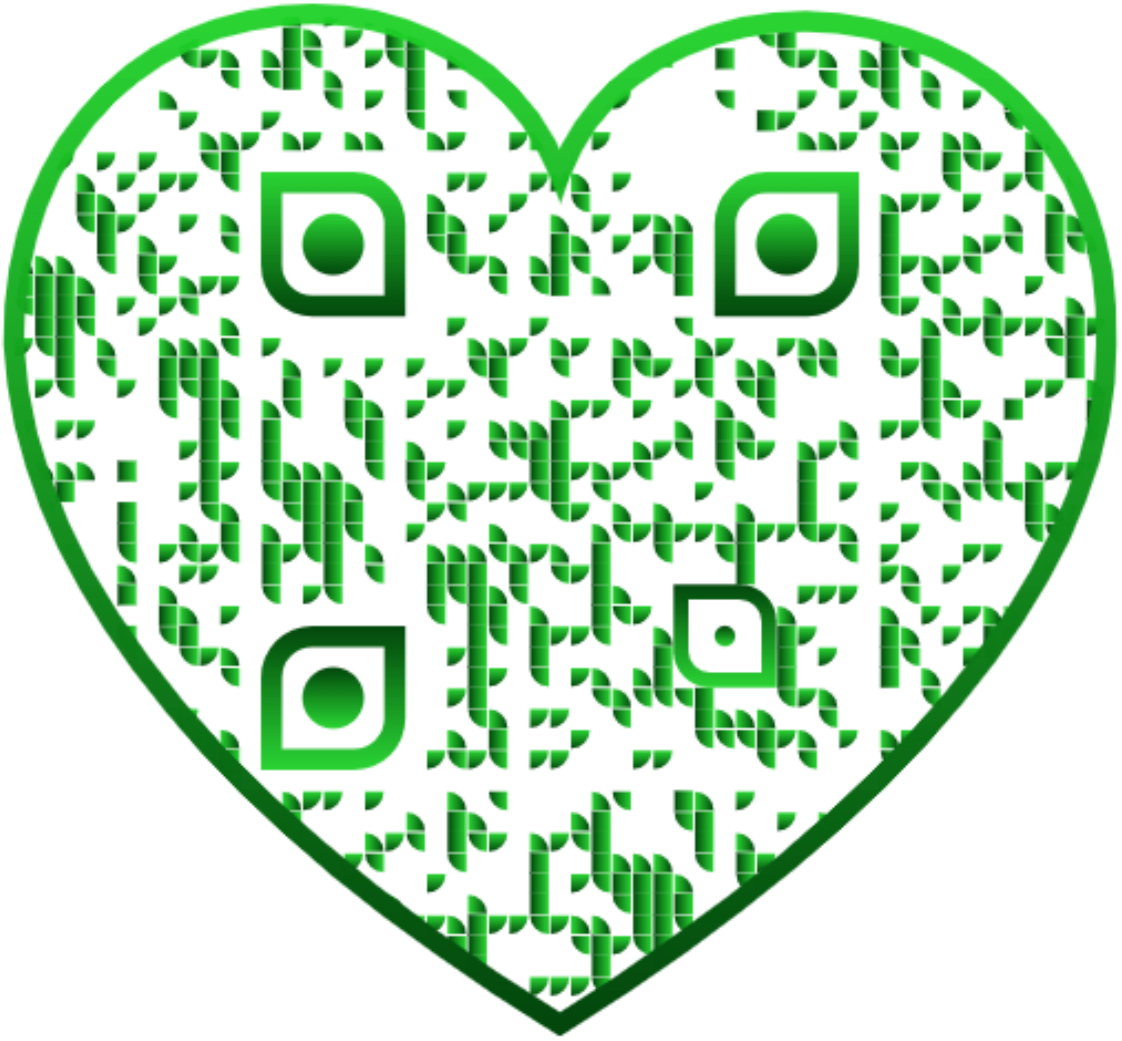
Estratégia Concursos

Informática para Caixa Econômica Federal - CEF (Técnico Bancário)

Prof. Diego Carvalho, Prof. Marcos Vinícius Alves Franco, Prof. Diego Carvalho

2 Redes de Computadores - Parte 2

Documento última vez atualizado em 27/01/2024 às 13:47.



Índice

) Redes de Computadores - Parte 2 - Noções Iniciais - Teoria

) Redes de Computadores - Parte 2 - Modelo OSI-ISO - Teoria

) Redes de Computadores - Parte 2 - Arquitetura TCP-IP - Teoria

) Redes de Computadores - Parte 2 - Principais Protocolos - Teoria

) Redes de Computadores - Parte 2 - Serviço VoIP - Teoria

) Redes de Computadores - Parte 2 - Resumo

) Mapa Mental - Redes de Computadores - Parte 2

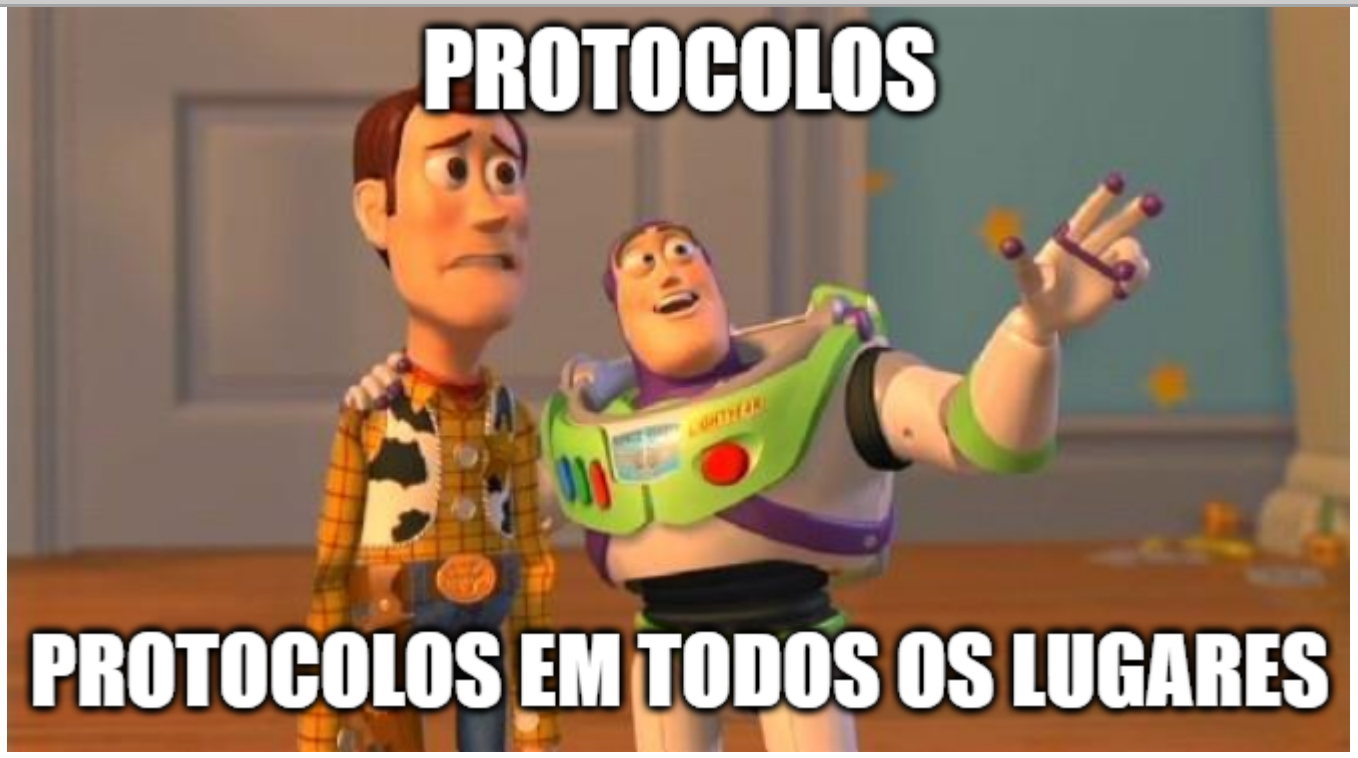
) Questões Comentadas - Redes de Computadores - Parte 2 - MULTIBANCAS

Redes de Computadores - Parte 2 - Noções Iniciais - Teoria

Apresentação da Aula

Fala, galera! O assunto da nossa aula de hoje é **Protocolos de Comunicação**! Pessoal, não há como se falar em redes de computadores como a internet sem falar sobre protocolos de comunicação. Para utilizar a Internet, você precisará dos protocolos IP, TCP ou UDP; para utilizar um navegador, você precisará dos protocolos HTTP, HTTPS e DNS; para enviar/receber e-mail, você precisará dos protocolos SMTP, POP3 ou IMAP; e assim por diante...

PROFESSOR DIEGO CARVALHO -www.instagram.com/professordiegocarvalho [1]



Galera, todos os tópicos da aula possuem Faixas de Incidência, que indicam se o assunto cai muito ou pouco em prova. *Diego, se cai pouco para que colocar em aula?* Cair pouco não significa que não cairá justamente na sua prova! A ideia aqui é: se você está com pouco tempo e precisa ver somente aquilo que cai mais, você pode filtrar pelas incidências média, alta e altíssima; se você tem tempo sobrando e quer ver tudo, vejam também as incidências baixas e baixíssimas. *Fechado?*

INCIDÊNCIA EM PROVA: baixíssima
INCIDÊNCIA EM PROVA: baixa
INCIDÊNCIA EM PROVA: média

INCIDÊNCIA EM PROVA: ALTA

INCIDÊNCIA EM PROVA: Altíssima

Além disso, essas faixas não são por banca – é baseado tanto na quantidade de vezes que caiu em prova independentemente da banca e também em minhas avaliações sobre cada assunto...

Protocolos de Comunicação de Comunicação

Conceitos Básicos

INCIDÊNCIA EM PROVA: BAIXA

PROTOCOLOS DE COMUNICAÇÃO

Protocolos são conjuntos de regras e convenções que especificam como os dispositivos em uma rede devem se comunicar. Eles definem os formatos dos dados, a sequência de mensagens, a detecção e correção de erros, o controle de acesso e muitos outros aspectos necessários para a comunicação eficaz entre computadores em uma rede. Esses protocolos desempenham um papel fundamental na garantia de que diferentes dispositivos de rede, com hardware e software diversos, possam se comunicar e trocar informações de maneira consistente.

Existe um renomado autor – chamado Andrew Tanenbaum – que afirma que "*um protocolo é um acordo entre as partes que se comunicam, estabelecendo como se dará a comunicação*". Outro grande autor – chamado Behrouz Forouzan – declara que um "*protocolo é um conjunto de regras que controlam a comunicação de dados*". **Já esse que vos escreve – chamado Diego Carvalho – gosta de pensar em protocolos simplesmente como um idioma.**

Questão

2023
2023
2023
4001426254

Nos itens que avaliem conhecimentos de informática, a menos que seja explicitamente informado o contrário, considere que: todos os programas mencionados estejam em configuração padrão, em português; o mouse esteja configurado para pessoas destras; expressões como clicar, clique simples e clique duplo refiram se a cliques com o botão esquerdo do mouse; e teclar corresponda à operação de pressionar uma tecla e, rapidamente, liberá la, acionando a apenas uma vez. Considere também que não haja restrições de proteção, de funcionamento e de uso em relação aos programas, arquivos, diretórios, recursos e equipamentos mencionados.

Acerca dos conceitos de redes de computadores, do programa de navegação Mozilla Firefox, em sua versão mais atual, e dos conceitos de organização e de gerenciamento de arquivos, julgue o item.

Um protocolo pode ser definido como um conjunto de regras e padrões que governa a comunicação entre os dispositivos em uma rede.

Solução

Gabarito: Certo.

Imagine que você está em um país estrangeiro e deseja se comunicar com os habitantes locais. Considere que você não conhece o idioma deles, e eles não conhecem o seu idioma. Para se entenderem, é necessário seguir regras específicas. Em uma rede de computadores, o idioma é como os dados são representados e organizados para a comunicação. Isso inclui a estrutura e a gramática usadas para transmitir informações de um dispositivo para outro.

Questão

|
|
2013 |
562664378

As regras e convenções usadas na comunicação das redes de computadores são conhecidas como:

A) conectores.

B) idiomas.

C) protocolos.

D) tradutores.

Solução

Gabarito: C) protocolos.

Regras e convenções usadas na comunicação de redes de computadores são chamadas de <u>protocolos</u> (Letra C).

Os protocolos de comunicação são como as regras que você segue para interagir com os habitantes locais. Eles definem como os dados são formatados, transmitidos e interpretados em uma rede. **Cada protocolo tem regras específicas, assim como diferentes idiomas têm suas próprias gramáticas e vocabulários.** Os dispositivos de rede, como computadores, roteadores e servidores, são como as pessoas que desejam se comunicar.

Eles precisam seguir as regras do protocolo para trocar informações com outros dispositivos na rede, da mesma forma que você segue as regras do idioma local para se comunicar com os habitantes locais. **Assim como você pode usar um intérprete ou um dicionário para traduzir seu idioma para o idioma local, os dispositivos de rede usam software e hardware para traduzir os dados do formato em que estão para o formato que os outros dispositivos entendem.**
Isso permite que diferentes dispositivos em uma rede se comuniquem, independentemente de suas diferenças de hardware ou software. **Em resumo, os protocolos de comunicação são como os idiomas que os dispositivos de rede usam para se entender.** Eles definem as regras para a transmissão de dados e permitem que diferentes dispositivos em uma rede se comuniquem, assim como seguir as regras de um idioma permite que você se comunique em um país estrangeiro.

Questão

| | 2010 | 373646995 |

Como são chamadas as regras da comunicação entre computadores em uma rede local?

A) Tipos

B) Limites

C) Postagem

D) Pilha

E) Protocolos

Solução

Gabarito: E) Protocolos

As regras de comunicação entre computadores em uma rede local são chamadas de <u>Protocolos</u> (Letra E).

Hoje em dia, existe um conjunto de protocolos padrão da internet chamado TCP/IP! Ele é a base da comunicação de redes na internet e fornece as regras e convenções que permitem que dispositivos em redes diferentes se comuniquem entre si de maneira eficaz. Não importa se é um notebook, um tablet ou um computador, também não importa se utiliza Linux ou Windows ou se possui arquitetura x86 ou x64. Se estiver conectado à Internet, estará utilizando o TCP/IP!

Redes de Computadores - Parte 2 - Modelo OSI-ISO - Teoria

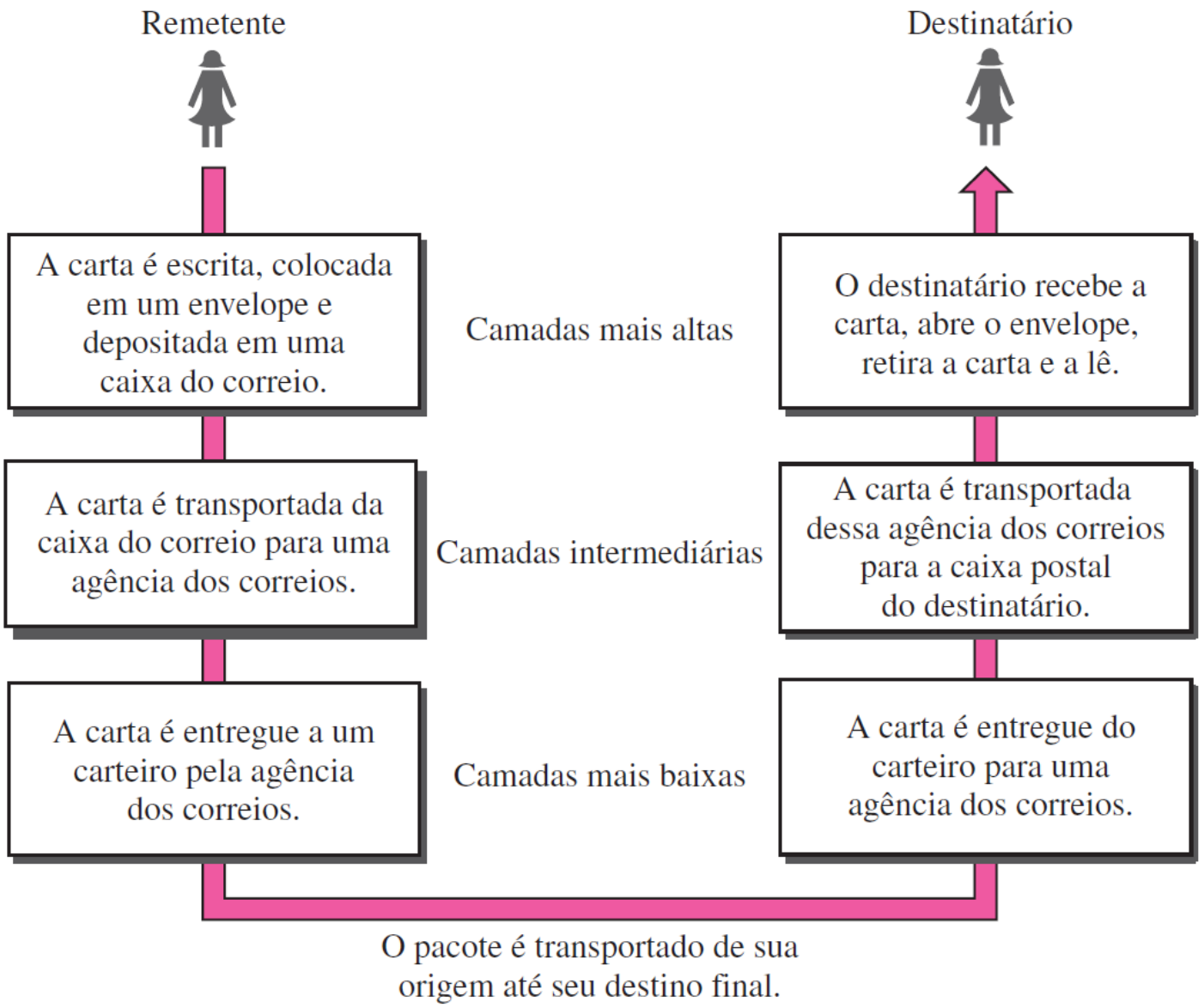
Modelo OSI/ISO

INCIDÊNCIA EM PROVA: MÉDIA

MODELO OSI/ISO
O Modelo OSI (*Open Systems Interconnection / International Organization for Standardization*) é um modelo de referência utilizado para entender como os protocolos de rede funcionam e interagem. Ele divide as funções de comunicação em uma rede de computadores em sete camadas, cada uma com um propósito específico. Essas camadas são organizadas hierarquicamente e servem como um guia para o desenvolvimento e a compreensão de protocolos de comunicação em redes.

Nós já sabemos que uma rede é uma combinação de hardware e software que envia dados de uma localidade para outra. **Para que dados possam trafegar de um ponto a outro, é necessário que tanto hardware quanto software realizem algumas tarefas.** *Pessoal, vocês já se perguntaram como um e-mail enviado para um amigo que mora do outro lado do mundo consegue chegar até o computador dele?* Tudo acontece tão rápido que até parece simples, mas não é!

Falando especificamente do contexto de softwares, a atividade de enviar um e-mail pode ser dividida em várias tarefas, cada uma das quais realizada por uma camada de software diferente.*Professor, não estou entendendo bulhufas!* Imaginem dois amigos se comunicando por cartas! *O processo de enviar uma carta a um amigo seria complexo se não existisse nenhum serviço disponível das agências dos correios, concordam?* Vejamos...



Na imagem anterior, temos um remetente, um destinatário e um transportador – provavelmente um carteiro. Olhando apenas para o lado do remetente, nós temos três tarefas que podem ser divididas em camadas; durante o transporte, a carta se encontra a caminho de seu destinatário (nesse momento, não nos interessa analisar as tarefas realizadas pelo transporte); por fim, ocorre de forma similar do lado direito, mas em ordem inversa.

De acordo com nossa análise, há três tarefas distintas no lado do remetente e outras três do destinatário, sendo que elas devem ser realizadas na sequência correta. **Note que cada camada no lado do remetente usa os serviços da camada imediatamente inferior.** O remetente na camada mais alta utiliza os serviços da camada intermediária; a camada intermediária usa os serviços da camada mais baixa; e a camada mais baixa utiliza os serviços do transportador.

A passagem de dados pelas camadas do dispositivo entre emissor e receptor é possível graças a uma interface entre cada par de camadas adjacentes. Cada interface define as informações e serviços que uma camada deve fornecer para a camada superior. **Desde que uma camada forneça os serviços esperados para a camada superior, a implantação específica de suas funções pode ser modificada ou substituída, sem exigir mudanças nas camadas adjacentes.**

Galera, dividir um problema em camadas com tarefas e serviços específicos é uma excelente estratégia para reduzir a complexidade de um problema. *Pois bem... e se eu dissesse para vocês que os engenheiros e cientistas pioneiros no estudo de redes de computadores decidiram utilizar essa mesma ideia?* A ISO (*International Standards Organization*) criou um modelo conceitual para auxiliar a compreender e projetar um modelo de redes de computadores:

Modelo OSI

(Open Systems Interconnection)

Esse modelo é considerado um modelo de sistema aberto. Ele foi projetado para promover a interoperabilidade entre diferentes sistemas de rede e fabricantes, permitindo que sistemas de diferentes origens se comuniquem de maneira eficaz. A ideia por trás de um sistema aberto é que ele não é restrito a uma única entidade ou fabricante, mas segue padrões abertos que são amplamente aceitos e seguidos pela indústria de tecnologia.

#VamosPraticar#

(QUADRIX / CAU-AP – 2021) Em redes de computadores, o modelo OSI é conhecido como sendo um "sistema fechado". É um modelo composto por três camadas e definido como um padrão que apenas um determinado fabricante pode utilizar.

Comentários: o Modelo OSI é considerado um "sistema aberto" e não é limitado a um único fabricante. Ele é um modelo de referência que foi desenvolvido para padronizar a comunicação de redes de computadores e permitir a interoperabilidade entre diferentes fabricantes e sistemas. Além disso, ele consiste em sete camadas e, não, em três. Cada camada desempenha um papel específico na comunicação de rede e é projetada para ser independente de implementações específicas. Isso garante que várias empresas possam seguir esse modelo e criar sistemas de rede compatíveis entre si (Errado).

#VamosPraticar#

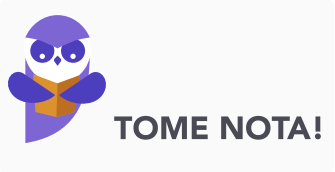
Isso possibilita a criação de redes em que dispositivos de diferentes fabricantes possam funcionar em conjunto de forma harmoniosa, seguindo as especificações do Modelo OSI.

numeração	CAMADA	Descrição	protocolos
7	APLICAÇÃO	Camada responsável por habilitar o usuário, seja ele humano ou software, a estabelecer a comunicação entre aplicações e a acessar a rede.	HTTP, SMTP, FTP, SSH, TELNET, SNMP, POP3, IMAP, DNS.
6	APRESENTAÇÃO	Camada responsável por definir o formato para troca de dados entre computadores, como se fosse um tradutor.	AFP, ICA, LPP, NCP, NDR, TOX, XDR, PAD.
5	SESSÃO	Camada responsável por permitir que duas ou mais aplicações em computadores diferentes possam abrir, usar e fechar uma conexão, chamada sessão.	NETBIOS.
4	TRANSPORTE	Camada responsável por organizar dados em segmentos e que eles cheguem ao destino livre de erros (sem perdas, sem duplicações e na ordem correta).	TCP, UDP, NETBEUI.
3	REDE	Camada responsável pelo endereçamento, roteamento e entrega de pacotes individuais de dados desde sua origem até o seu destino, provavelmente através de várias redes.	IP, ICMP, ARP RARP, NAT.
2	ENLACE	Camada responsável por organizar os dados em frames (ou quadros) e por estabelecer uma conexão nó-a-nó entre dois dispositivos físicos que compartilham o mesmo meio físico.	Ethernet, Token Ring, Bluetooth, Wi-Fi.

1	FÍSICA	Camada responsável por definir as especificações elétricas e físicas da conexão de dados.	USB, DSL.

MNEMÔNICO das camadas [2]						
F	E	R	T	S	A	A
FÍSICA	ENLACE	REDE	TRANSPORTE	SESSÃO	APRESENTAÇÃO	APLICAÇÃO
FLAMENGO	ENSACOU NA	REDE	TRÊS	SAPECADAS NO	ATLÉTICO E	avaí

O Modelo OSI é basicamente um modelo de referência para conexão e projetos de sistemas de redes que se baseia em camadas sobrepostas. Sendo beeeeeeem rigoroso, esse modelo não é propriamente dito uma arquitetura de rede, uma vez que não especifica os serviços e os protocolos exatos que devem ser utilizados em cada camada. Em outras palavras, nem sempre será possível "encaixar" um protocolo em uma camada específica do Modelo OSI.



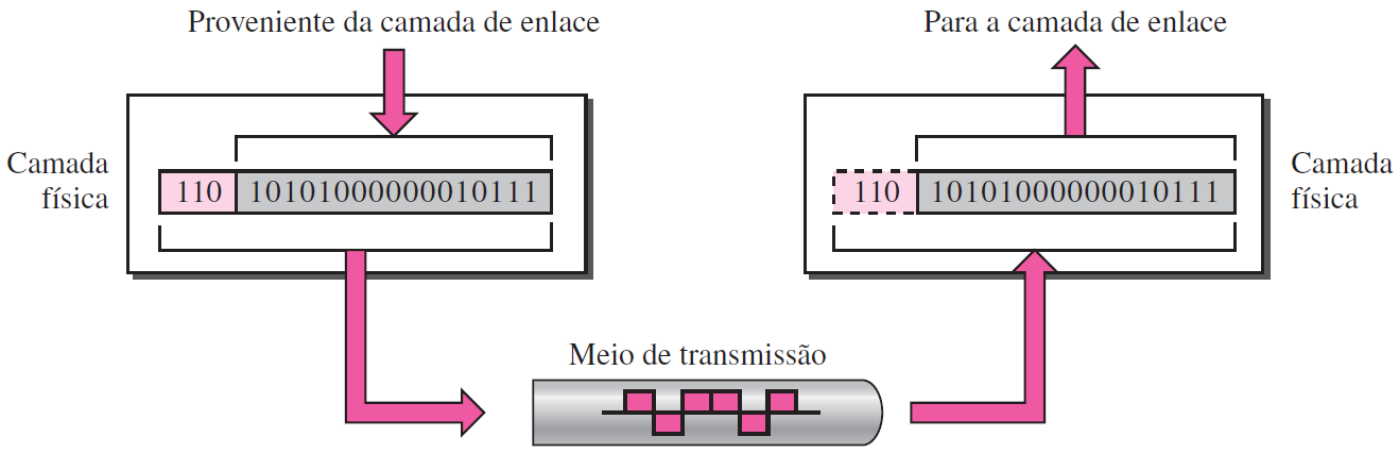
Esse modelo é apenas uma abstração teórica – uma referência conceitual – usado pela academia para representar o que seria um modelo perfeito de rede com suas respectivas descrições de camadas. Ele tem uma função mais didática do que pragmática. Não se trata de um modelo utilizado atualmente em redes de computadores – na prática, a arquitetura utilizada atualmente é o TCP/IP.

Nós sabemos que a comunicação entre dois computadores é extremamente complexa, logo esse modelo sugere dividir essa complexidade em uma estrutura de sete camadas distintas, porém relacionadas entre si, cada uma das quais definindo uma parte do processo de transferência de informações através de uma rede. **Compreender esses conceitos é importante para entender posteriormente a função de cada protocolo.** Nos tópicos

seguintes, nós veremos a função de cada uma dessas camadas. Vem comigo... é legal! Eu juro... no fim da aula, tudo fará sentido!

Camada Física

A camada física coordena as funções necessárias para transportar um fluxo de bits através de um meio físico. Ela trata das especificações mecânicas e elétricas da interface e do meio de transmissão e também define os procedimentos e funções que os dispositivos físicos e interfaces têm de executar para que a transmissão seja possível. A imagem seguinte mostra a posição da camada física em relação ao meio de transmissão e a camada de enlace.



Imagine-a como a infraestrutura física de um restaurante (Ex: prédio, encanamentos, rede elétrica). Ela garante que o local esteja funcionando e possua infraestrutura adequada para receber clientes.

Características da CAMADA FÍSICA
Responsável por definir as especificações dos meios de transmissão, como sinais elétricos, ópticos ou de rádio.
Responsável por definir as especificações físicas dos dispositivos de rede, como cabos, conectores e transceptores.

Responsável por definir como os bits serão codificados para serem transmitidos como sinais elétricos, ópticos, etc.
Responsável por definir o sentido das transmissões entre dois dispositivos: simplex, Half-duplex ou full-duplex.
Responsável por descrever a topologia da rede, ou seja, como os dispositivos estão fisicamente conectados.
Responsável por transmitir e recepcionar bits brutos.
Responsável por definir os níveis de voltagem, frequência e modulação para a transmissão de dados.
Essa camada não se preocupa com o conteúdo dos dados, apenas com sua transmissão física.

#VamosPraticar#

(CESPE / FUB – 2022) A camada física do modelo OSI trata da transmissão de bits normais dos conectores para conexões de rede.

Comentários: essa camada trata de como os dados são fisicamente transmitidos por meio de meios de transmissão, como cabos, fibras ópticas, **conectores**, sinais elétricos ou ondas de rádio (Correto).

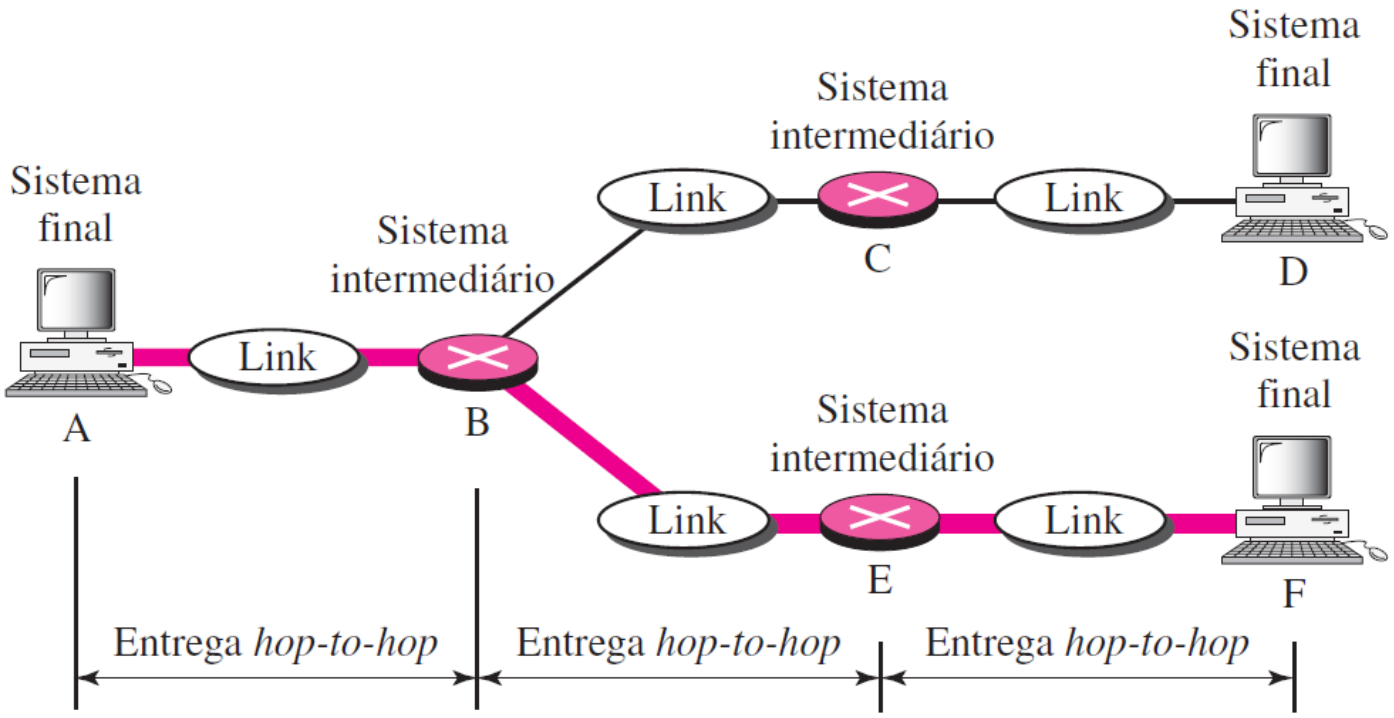
(QUADRIX / CRA-BA – 2021) Em redes de computadores, uma das funções da camada física do modelo OSI é determinar as características mecânicas das placas de rede e dos dispositivos.

Comentários: a camada física define especificações elétricas e físicas dos dispositivos. Em especial, define a relação entre um dispositivo e um meio de transmissão, tal como um cabo de cobre ou um cabo de fibra óptica (incluindo layout de pinos, tensões, impedância da linha, especificações do cabo, temporização, hubs, repetidores, adaptadores de rede, etc) (Correto).

#VamosPraticar#

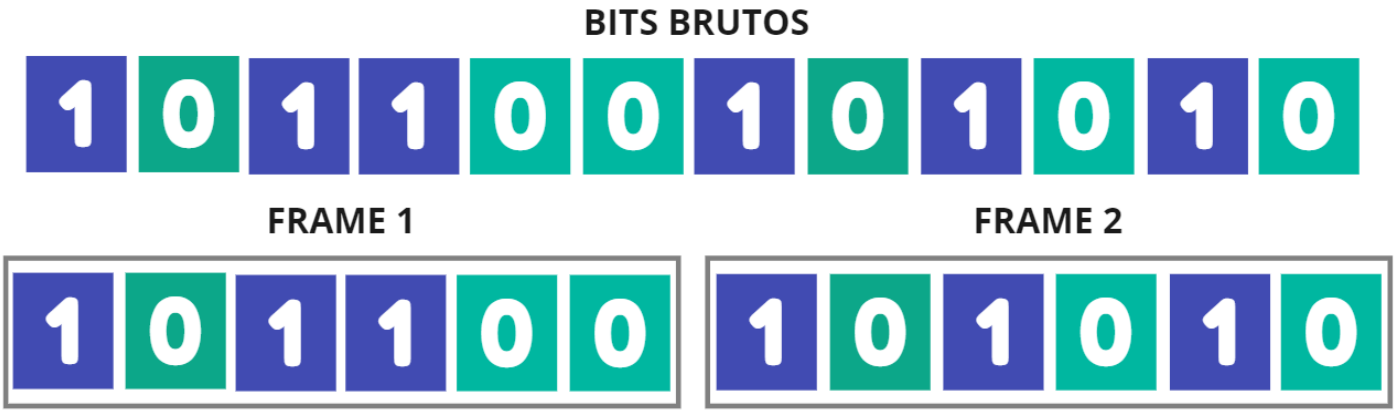
Camada de Enlace

A camada de enlace de dados transforma a camada física de um meio de transmissão bruto em um link confiável. Ela faz que a camada física pareça livre de erros para a camada superior (a camada de rede). Ela oferece diversos serviços: empacotamento de bits em quadros (ou *frames*); oferecer um endereçamento físico; realizar o controle de fluxo, controle erros, correção de erros, controle acesso; etc. Vamos analisar a imagem abaixo para entender como essa camada funciona:



A comunicação na camada de enlace de dados ocorre entre dois nós adjacentes. **Note que, para enviar dados de A a F, são feitas três entregas parciais.** Primeiro, a camada de enlace de dados em A envia um frame para a camada de enlace de dados em B (um roteador). Segundo, a camada de enlace de dados em B envia um novo frame à camada de enlace em E. Finalmente, a camada de enlace em E envia um novo frame à camada de enlace em F.

A imagem apresentada a seguir representa como essa camada empacota conjuntos de bits no que chamamos de quadros (ou *frames*). Vejamos:



Agora vamos detalhar um pouco mais três serviços oferecidos por essa camada: controle de fluxo, controle de erros e controle de acesso:

- **Controle de Fluxo:** se a velocidade na qual os dados são recebidos pelo receptor for menor que a velocidade na qual os dados são transmitidos pelo emissor, a camada de enlace de dados impõe um mecanismo de controle de fluxo para impedir que o receptor fique sobrecarregado.

Um método para implementar o controle de fluxo são as **Janelas Deslizantes**. Nele, o destinatário informa ao remetente quantos dados ele pode receber de uma vez. O remetente então ajusta a taxa de transmissão para garantir que não envie mais dados do que a capacidade disponível. O controle de fluxo envolve também o recebimento e a confirmação de pacotes. O destinatário informa ao remetente quais pacotes foram recebidos com sucesso e quais precisam ser retransmitidos.

Imagine que você é um garçom em um restaurante movimentado, e sua tarefa é entregar pratos de comida às mesas dos clientes. O restaurante tem uma regra: você só pode carregar até três pratos de uma vez. Isso evita que você sobrecarregue e derrube comida pelo caminho. Se você seguir essa regra, a entrega dos pratos será eficiente e sem acidentes. **Isso se assemelha ao controle de fluxo, em que o remetente ajusta a taxa de transmissão para não sobrecarregar o destinatário.**

- **Controle de Erros:** essa camada adiciona mecanismos para detectar e retransmitir frames danificados ou perdidos e também usa mecanismos para reconhecer frames duplicados. Em geral, o controle de erros é obtido por meio de bits acrescentados ao final do quadro.

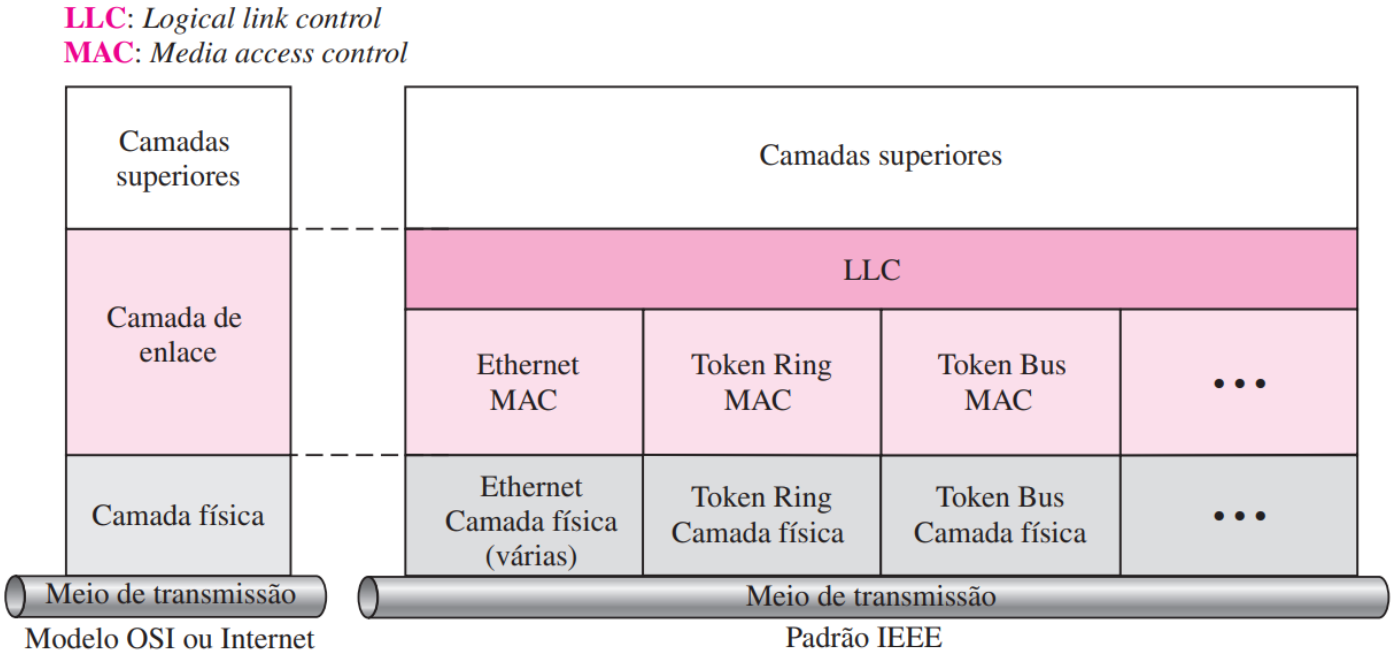
A camada de enlace é responsável por fornecer mecanismos de detecção de erros. Nesse sentido, ela garante que os dados sejam transmitidos de forma confiável entre dispositivos diretamente conectados, mas se ocorrerem erros durante a transmissão, ela pode detectá-los. **Essa camada é capaz de identificar erros – causados, por exemplo, por ruídos eletromagnéticos ou atenuação de sinal – através de diversas técnicas (Ex: CRC, Verificação de Paridade, Checksum, etc).**

Quando o quadro é recebido, o dispositivo de destino verifica – por meio de alguma das técnicas mencionadas no parágrafo anterior – se ocorreram erros durante a transmissão de dados. **Se um erro for detectado, o quadro pode ser descartado ou sua retransmissão pode ser solicitada.** Para corrigir os erros detectados, também existem diversas técnicas (que não entraremos em detalhes devido à sua complexidade). Voltando à nossa analogia...

Às vezes, ao entregar pratos, você (que é o garçom) pode escorregar e deixar cair um prato no chão. Para garantir que o erro seja corrigido, você verifica com o chef de cozinha se pode buscar outro prato para substituir o quebrado. Isso é semelhante ao controle de erros na camada de enlace, **onde são usados mecanismos, como a verificação de paridade, para detectar e corrigir erros nos dados transmitidos.**

- **Controle de Acesso:** quando dois ou mais dispositivos estiverem conectados ao mesmo link, são necessários protocolos da camada de enlace de dados para determinar qual dispositivo assumirá o controle do link em dado instante.

Essa camada possui duas subcamadas: Camada LLC (Logical Link Control) e Camada MAC (Media Access Control). A primeira subcamada é responsável pelos controles de fluxo e erros, abstraindo a subcamada MAC; e a segunda é responsável pelo controle de acesso múltiplo, definindo métodos de acesso específicos para diferentes tipos de redes locais (Ex: CSMA/CD para Ethernet; Tokens para Token Ring; etc).



#VamosPraticar#

(FCC / AL-AP – 2020) A camada de enlace IEEE Ethernet assegura que os dados sejam transmitidos ao equipamento apropriado e faz a ponte entre a camada de rede e a camada física. Essa camada possui as subcamadas:

a) Logical Link Control – LLC e Media Access Control – MAC.

b) Integrated Service Digital – ISD e Digital Subscriber Line – DSL.

c) Network Address Translation – NAT e Logical Link Control – LLC.

d) Synchronous Optical Control – SOC e Media Access Control – MAC.

e) Synchronous Digital Hierarchy – SDH e Fiber Distributed Data Interface – FDDI.

Comentários: conforme acabamos de estudar, as subcamadas são LLC e MAC (Letra A).

#VamosPraticar#

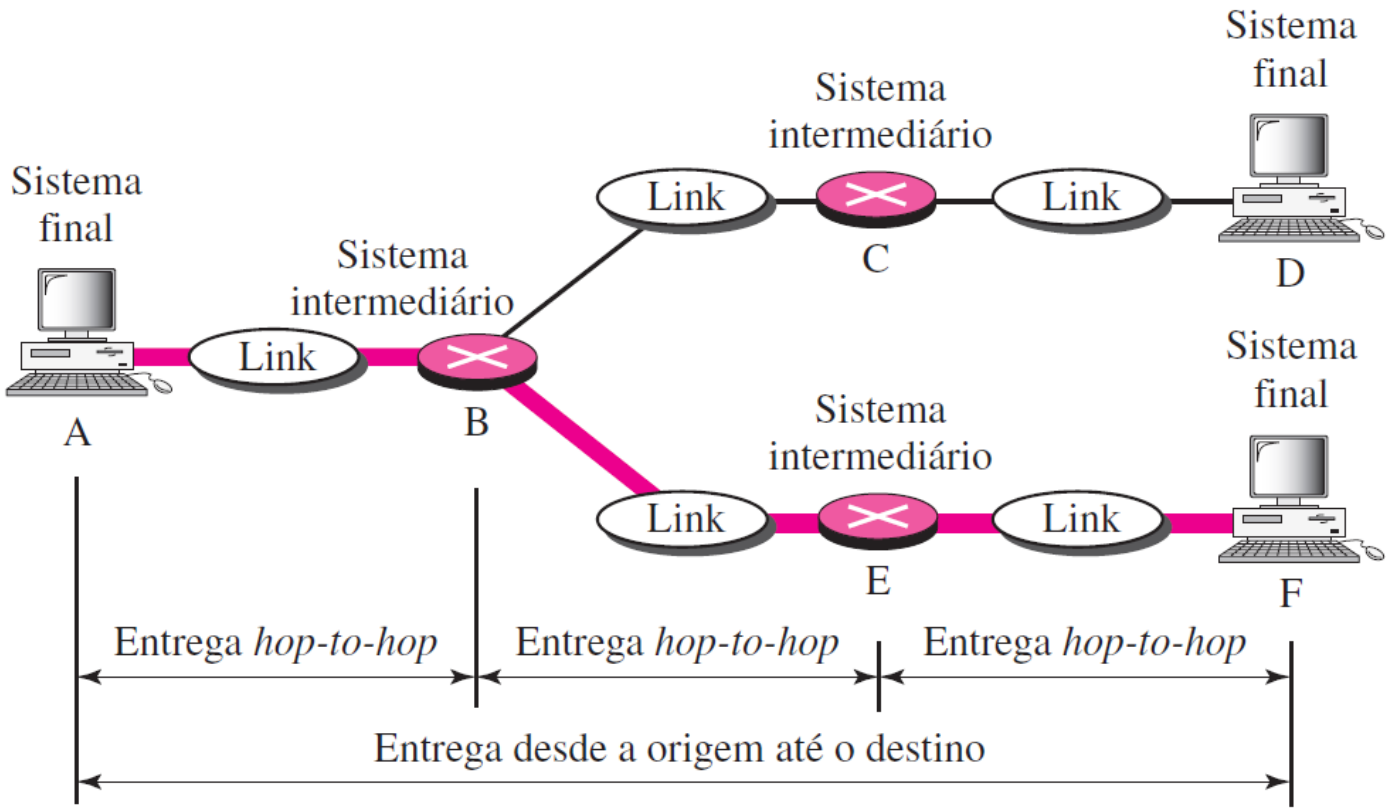
Voltando à nossa analogia: no restaurante, a cozinha pode atender vários garçons, mas é necessário um sistema de controle de acesso para garantir que todos os garçons não entrem na cozinha ao mesmo tempo, o que poderia causar confusão. **Cada garçom deve esperar sua vez na porta da cozinha.** Isso é análogo ao controle de acesso na camada de enlace, onde dispositivos competem para acessar o meio de transmissão, garantindo que apenas um dispositivo transmita por vez.

Características da CAMADA de enlace
Responsável pela comunicação direta entre dispositivos adjacentes na mesma rede local.
Responsável por fornecer mecanismos de detecção e correção de erros.
Responsável por controlar o acesso ao meio compartilhado, quando necessário.
Responsável por define os endereços físicos dos dispositivos na rede (Endereço MAC).
Responsável por realizar o controle de fluxo e acesso à camada de enlace.
É dividida em duas subcamadas: LLC (Camada de Controle Lógico) e MAC (Controle de Acesso ao Meio).

Camada de Rede

A camada de rede é responsável pela entrega de um pacote desde sua origem até o seu destino, possivelmente através de várias redes. Embora a camada de enlace coordene a entrega do pacote entre dois sistemas na mesma rede, a camada de rede busca transmitir cada pacote de seu ponto de origem até seu destino final. Se dois sistemas estiverem conectados ao mesmo link, em geral não há a necessidade de uma camada de rede.

Entretanto, se dois sistemas estiverem conectados a redes diferentes por meio de dispositivos intermediários de conexão entre as redes (como roteadores), normalmente, há a necessidade da camada de rede para realizar a entrega da origem até o destino. **Essa camada é responsável pela entrega de pacotes individuais de dados desde o host (máquina) de origem até o host de destino.** Além disso, é responsável pelo endereçamento lógico e pelo roteamento. Vejamos como:



Note que agora precisamos de uma entrega desde a origem até o destino. A camada de rede em A envia o pacote para a camada de rede em B. Quando o pacote chega no roteador B, este toma uma decisão baseado no destino final (F) do pacote. O roteador B usa sua tabela de roteamento para descobrir que o próximo nó é o roteador E. Logo, a camada de rede em B envia o pacote para a camada de rede em E, que – por sua vez – envia o pacote para a camada de rede em F.

A imagem apresentada a seguir representa como essa camada empacota conjuntos de frames no que chamamos de pacotes (ou *packets*). Vejamos:

O endereçamento físico (Endereço MAC) implementado na camada de enlace trata do problema de endereçamento localmente. Se um pacote ultrapassar os limites da rede, precisaremos de um outro sistema de endereçamento para ajudar a distinguir os sistemas de origem e destino. **A camada de rede adiciona um cabeçalho ao pacote proveniente da camada superior que, entre outras coisas, inclui o endereçamento lógico (Endereço IP) do emissor e do receptor.**

Em nossa analogia, imagine que o restaurante faz parte de uma grande franquia e precisa estar coordenado com outros restaurantes da mesma rede. A camada de rede é como o serviço que roteia os insumos para a produção dos pratos do restaurante entre os diferentes restaurantes da franquia, garantindo que eles tenham a matéria prima para a produção dos pratos, mesmo que eles estejam em locais diferentes.

Características da CAMADA de rede
Responsável pelo roteamento, permitindo que pacotes sejam enviados da origem ao destino em redes distintas.
Responsável por definir os endereços lógicos dos dispositivos na rede, como os endereços IP.
Responsável por realizar o controle de congestionamento e encaminhamento dos pacotes de dados.
Responsável por dividir pacotes longos em fragmentos menores para transmissão e reagrupá-los no destino.
Responsável por implementar tabelas de roteamento para decidir o melhor caminho para encaminhar os pacotes.

#VamosPraticar#

(CESPE / PETROBRÁS – 2022) A principal função da camada de transporte no modelo OSI é fazer o redirecionamento dos pacotes entre redes diferentes.

Comentários: a camada de transporte lida com questões como controle de fluxo, correção de erros e garantia de entrega confiável. A função de redirecionamento de pacotes entre redes diferentes é atribuída à camada de rede (Errado).

#VamosPraticar#

Camada de Transporte

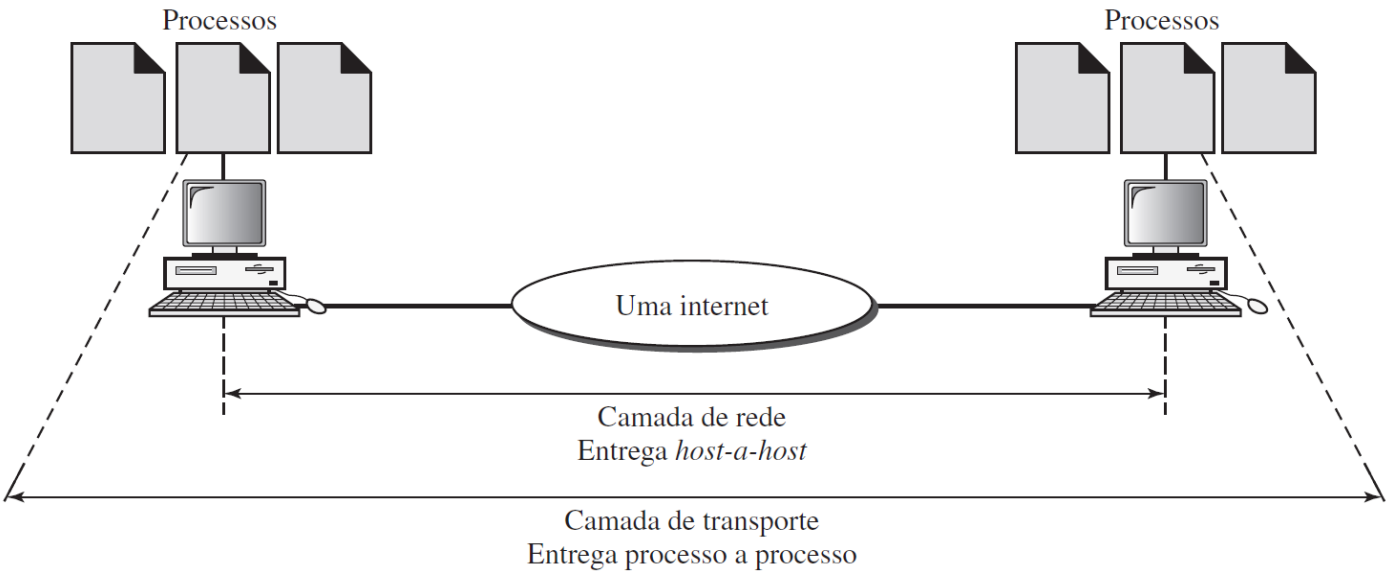
A camada de transporte é responsável pela entrega processo a processo de toda a mensagem. Processo é a instância de uma aplicação que está sendo executada em uma máquina. Embora a camada de rede supervisione a entrega da origem ao destino dos pacotes individuais, ela não reconhece qualquer relação entre esses pacotes. Ela trata cada um deles independentemente, como se cada trecho pertencesse a uma mensagem separada, ocorra isto ou não.

Normalmente, computadores executam vários programas ao mesmo tempo. Logo, a entrega origem-ao-destino significa a entrega não apenas de um computador para o seguinte, mas também de um processo específico (programa em execução) em um computador para um processo específico no outro. **A camada de rede encaminha cada pacote para o computador correto; a camada de transporte leva a mensagem inteira para o processo correto naquele computador.**

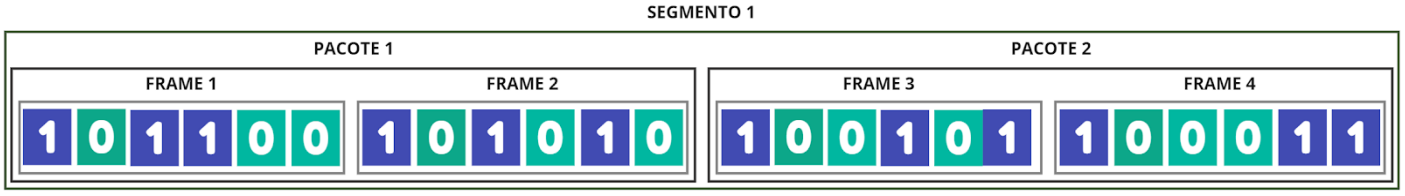
Na camada de transporte, uma mensagem é dividida em segmentos transmissíveis, com cada segmento contendo um número de sequência. **Esses números permitem à camada de transporte remontar a mensagem corretamente após a chegada no destino e identificar e substituir pacotes que foram perdidos na transmissão.** Ela também pode ser tanto orientada à conexão como não. *Como assim, Diego?*

Uma camada de transporte não orientada à conexão trata cada segmento como um pacote independente e o entrega à camada de transporte na máquina de destino. Uma camada de transporte orientada à conexão estabelece em primeiro lugar uma conexão com a camada de transporte na máquina de destino antes de iniciar a entrega dos pacotes. **Após todos os dados serem transferidos a conexão é encerrada.**

A camada de transporte também responsável por garantir que a mensagem chegue intacta e na sequência correta, supervisionando tanto o controle de erros como o controle de fluxo no nível origem-destino. *Professor, a camada de enlace já não fazia um controle de erros e fluxo?* **Sim, mas ela fazia no nível nó e nó adjacente; aqui ocorre no nível origem-destino.** A imagem seguinte apresenta o funcionamento da comunicação na camada de transporte:

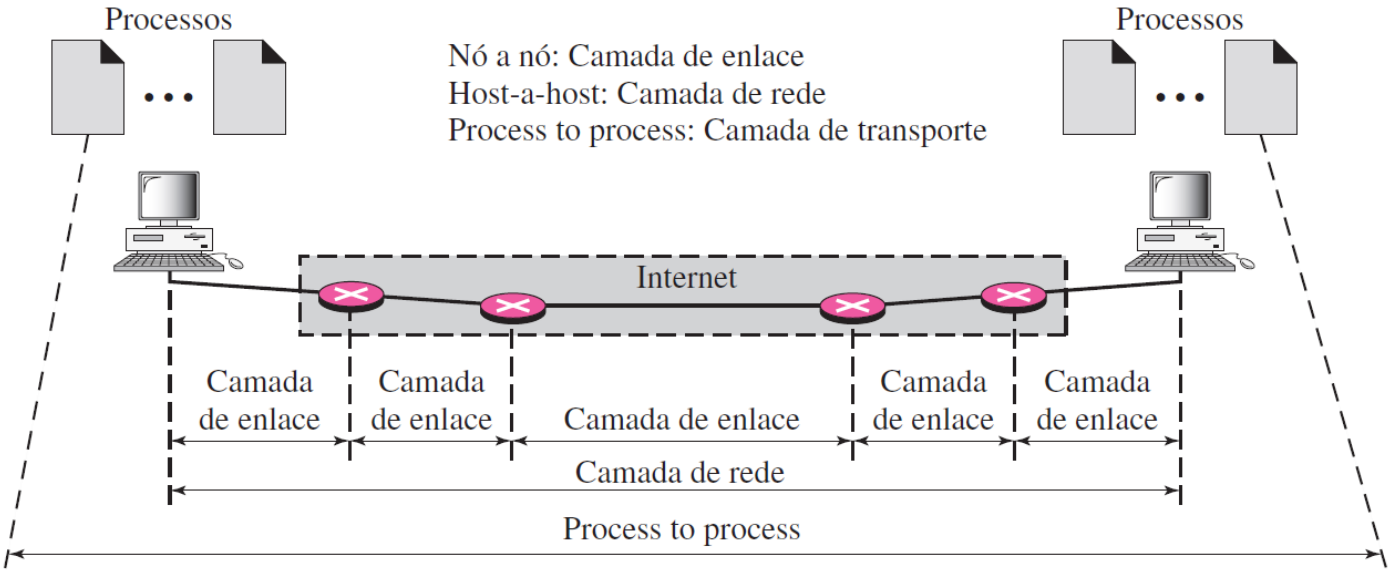


A imagem apresentada a seguir representa como essa camada empacota conjuntos de pacotes no que chamamos de segmentos (ou *segments*). Vejamos:



Sendo rigoroso com a nomenclatura utilizada (e as bancas, infelizmente, nem sempre são), existem três tipos de comunicação diferentes:

TIPOS DE COMUNICAÇÃO	DESCRIÇÃO
NÓ A NÓ	Também chamada de comunicação ponto-a-ponto ou comunicação hop-a-hop, conecta um dispositivo intermediário a outro dispositivo intermediário adjacente. Trata-se do tipo de comunicação realizada na camada de enlace.
HOST A HOST	Conecta uma máquina a outra, ignorando dispositivos intermediários. Trata-se do tipo de comunicação realizada na camada de rede (Obs: autores divergem nesse ponto, alguns afirmam que a camada de rede também se comunica nó a nó).
FIM A FIM	Também chamada de comunicação processo-a-processo ou comunicação ponta-a-ponta, conecta processos ou aplicações rodando em duas máquinas. Trata-se do tipo de comunicação realizada na camada de transporte.



Voltando à nossa analogia: **esta camada é como o serviço de entregadores que leva os pedidos dos restaurantes aos clientes em suas em suas casas.** Ela garante que os pedidos sejam divididos em pacotes menores, para que possam ser transportados de forma eficiente e sejam entregues com sucesso. Galera, eu tento fazer analogias para que vocês entendam melhor, mas toda analogia tem a sua limitação. Se não compreenderam por meio da analogia, apenas ignorem.

Características da CAMADA de transporte
Responsável por fornecer comunicação processo a processo entre dois dispositivos em diferentes sistemas finais.
Responsável pela segmentação e reagrupamento de dados em pacotes ou segmentos para a transmissão.
Oferece controle de fluxo para garantir que dispositivos transmitam dados em uma taxa compatível.
Responsável por realizar a multiplexação e os segmentos sejam identificados corretamente no destino.
Fornece detecção de erros e retransmissão de pacotes perdidos ou corrompidos, quando necessário.
Responsável por implementar os protocolos de transporte, como TCP e UDP.

#VamosPraticar#

(VUNESP / Prefeitura de Ilhabela-SP – 2020) No modelo de referência OSI, a Camada de Transporte é responsável pelo envio dos dados recebidos pela Camada de Sessão para a Camada de Rede,

a) fornecendo o roteamento de quadros entre redes e o controle de tráfego da sub-rede.

b) garantindo a entrega sem erros, em sequência e sem perdas ou duplicações.

c) sem a sua divisão em pacotes, que será feita pela camada subsequente.

d) sem garantia de que não haja perdas ou duplicações de pacotes.

e) sendo também responsável por iniciar e encerrar conexões de rede.

Comentários: (a) Errado, essa é uma responsabilidade da camada de rede; (b) Correto, a camada de transporte fornece os mecanismos de controle de fluxo e correção de erros para assegurar a integridade da comunicação entre as camadas de transporte nos dispositivos finais; (c) Errado, essa é uma responsabilidade da camada de rede; (d) Errado, há controle de perdas e duplicações de pacotes; (e) Errado, essa é uma responsabilidade da camada de sessão (Letra B).

#VamosPraticar#

Camada de Sessão

Essa camada é responsável por permitir que duas ou mais aplicações em computadores diferentes possam abrir, usar e fechar uma conexão, chamada sessão. Ela gerencia a comunicação para que, caso haja alguma interrupção, ela possa ser reiniciada do ponto da última marcação recebida. Essa camada controla o diálogo da rede – estabelecendo, mantendo e sincronizando a interação entre sistemas que se comunicam.

Essa camada possibilita a dois sistemas estabelecerem um diálogo, permitindo que a comunicação entre dois processos ocorra em modo half ou full-duplex. Ela também permite que um processo adicione **pontos de verificação/sincronização**, ao fluxo de dados. Exemplo: se um sistema estiver enviando um arquivo de 2.000 páginas, é recomendável inserir esses pontos a cada 100 páginas para garantir que cada unidade de 100 páginas foi recebida e confirmada de forma independente.

Nesse caso, se ocorrer uma falha durante a transmissão da página 523, as únicas páginas que precisarão ser reenviadas após a recuperação do sistema serão as páginas 501 a 523. As páginas anteriores à página 501 não precisarão ser reenviadas. Voltando à analogia: imagine que os clientes estejam se reunindo em grupos para comer juntos no restaurante. **A camada de**

sessão ajuda a coordenar essas reuniões, garantindo que todos tenham a mesma experiência de jantar.

Características da CAMADA de sessão
Responsável pelo estabelecimento, gerenciamento e encerramento de sessões de comunicação entre dispositivos.
Controla o diálogo entre aplicativos em sistemas finais e coordena as interações entre eles.
Realiza a sincronização dos dados, garantindo que eles sejam transmitidos de forma ordenada e sem duplicações.
Responsável por fornecer serviços para garantir que a comunicação possa ser retomada após uma interrupção.
Responsável por lidar com a detecção e correção de erros relacionados à sequência de mensagens.
Responsável por implementar mecanismos de controle de diálogo, como controle de turnos e controle de token.

Camada de Apresentação

A camada de apresentação é responsável pela sintaxe e semântica das informações trocadas entre dois sistemas. Essa camada também é responsável pela tradução, compressão e criptografia dos dados – além de estabelecer formato para troca de dados entre computadores. Ela cuida das diferenças sintáticas na representação de dados. Um exemplo de um serviço de apresentação seria a conversão de dados codificados em EBCDIC para dados codificados em ASCII.

Normalmente, processos (programas em execução) em dois sistemas em geral trocam informações na forma de *strings* (sequências de caracteres), números, entre outros. As informações têm de ser convertidas em fluxos de bits antes de serem transmitidas. **Como diferentes computadores utilizam sistemas de codificação diferentes, a camada de apresentação é a camada responsável pela interoperabilidade entre esses métodos de codificação diferentes.**

A camada de apresentação no emissor traduz as informações de um formato específico do emissor em um formato comum. A camada de apresentação no receptor traduz o formato comum em um formato específico do receptor. *E quando temos que transmitir informações confidenciais?* Um sistema deve ser capaz de garantir privacidade! **A criptografia significa que o emissor converte as informações originais em um outro formato e envia a mensagem resultante pela rede.**

A descriptografia reverte o processo original convertendo a mensagem de volta ao seu formato original. **Por fim, a compressão de dados reduz o número de bits contidos nas informações.** Ela se torna particularmente importante na transmissão de conteúdos multimídia, como texto, áudio e vídeo. Voltando à nossa analogia do restaurante: às vezes, as pessoas têm preferências específicas sobre como a comida é apresentada.

A camada de apresentação garante que os pratos sejam servidos da maneira que os clientes desejam, seja com enfeites especiais ou embalagens diferenciadas.

Características da CAMADA de apresentação
Responsável pela tradução, compressão e criptografia dos dados que serão transmitidos na rede.
Lida com questões de representação dos dados, como codificação de caracteres e formatação de dados.
Garante a interoperabilidade entre diferentes sistemas, permitindo a comunicação em diferentes formatos.
Realiza a compressão de dados para otimizar a eficiência da transmissão.
Pode criptografar os dados para fornecer segurança durante a transmissão.
Lida com a detecção e correção de erros de representação de dados.

#VamosPraticar#

(UFMT / UFMT – 2021) Assinale a alternativa que apresenta a camada do modelo OSI que está relacionada à sintaxe e à semântica das informações transmitidas, tornando possível a comunicação entre computadores com diferentes representações internas dos dados.

a) Camada de sessão

b) Camada de apresentação

c) Camada de transporte

d) Camada de aplicação

Comentários: a camada de apresentação está relacionada à sintaxe e à semântica das informações transmitidas, permitindo a comunicação entre computadores com diferentes representações internas dos dados. Ela lida com funções como tradução de formatos de dados, criptografia e compressão (Letra B).

(FEPESE / Companhia Águas de Joinville – 2023) Qual camada do modelo OSI é responsável pela tradução, criptografia e compactação dos dados?

a) camada de aplicação

b) camada de enlace

c) camada de sessão

d) camada de transporte

e) camada de apresentação

Comentários: a camada de apresentação é responsável por traduzir, criptografar e compactar os dados de acordo com as necessidades da aplicação e da rede. Isso significa que ela lida com a sintaxe e a semântica das informações transmitidas, permitindo a comunicação entre computadores com diferentes representações internas dos dados (Letra E).

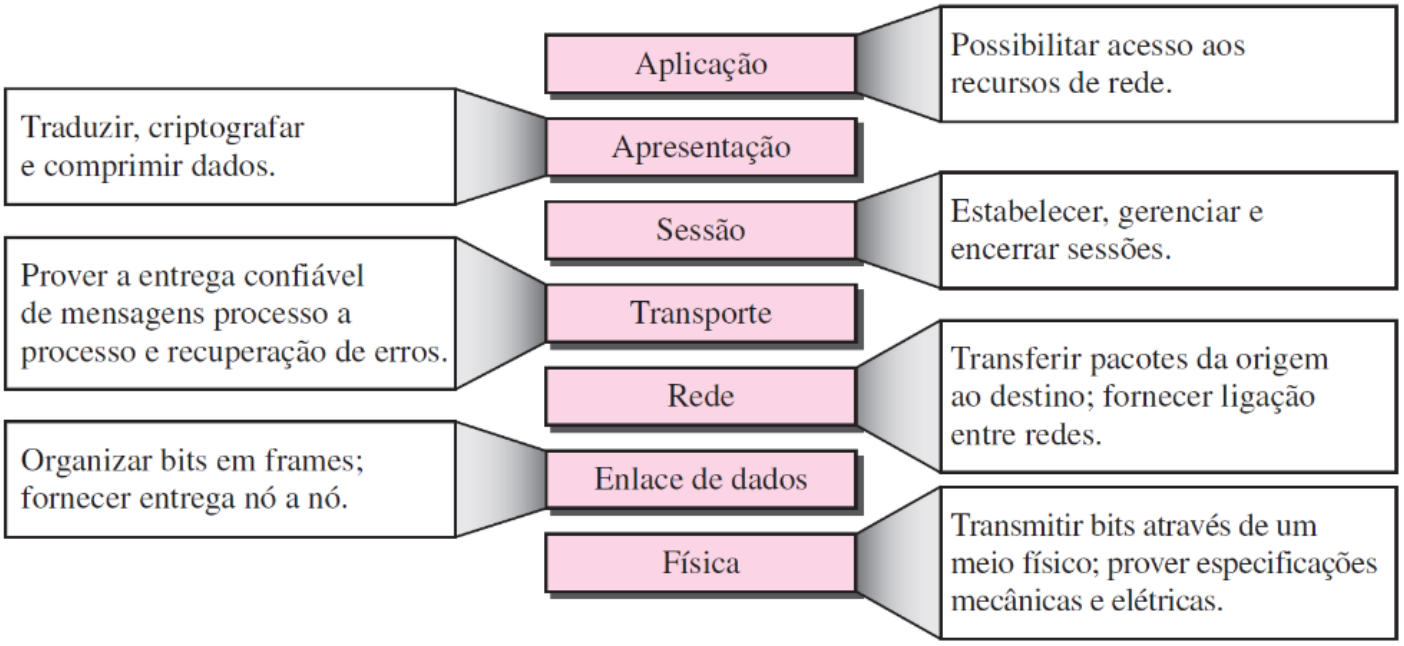
#VamosPraticar#

Camada de Aplicação

A camada de aplicação habilita o usuário, seja ele humano ou software, a acessar a rede. Ela fornece interface com o usuário e suporte a serviços, como e-mail, acesso e transferência de arquivos remotos, gerenciamento de bancos de dados compartilhados e outros tipos de serviços de informação distribuídos. Em suma: essa camada é responsável por prover serviços ao usuário. Voltando à nossa analogia do restaurante...

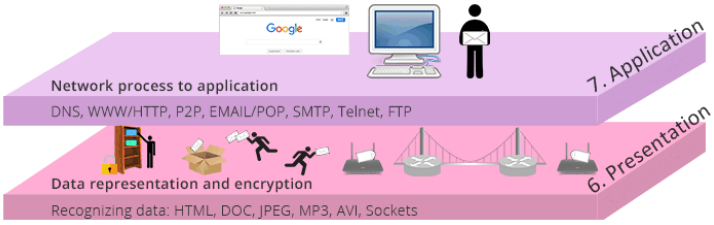
A camada de aplicação é como o cardápio do restaurante. Ela oferece uma variedade de opções aos clientes, como diferentes pratos e bebidas, permitindo que eles escolham o que desejam.

Características da CAMADA de aplicação
Responsável por fornecer serviços de rede diretos aos aplicativos do usuário final.
Envolve aplicativos de software, como navegadores, clientes de e-mail, e outros programas que utilizam a rede.
Fornecimento de uma interface entre o aplicativo do usuário e as camadas inferiores do Modelo OSI.
Implementa protocolos específicos de aplicação (Ex: HTTP para web e SMTP para e-mails).
Realiza a comunicação com os aplicativos de usuário final, traduzindo os comandos e solicitações dos aplicativos.
Fornecimento de serviços de aplicação (Ex: autenticação, transferência de arquivos, acesso a bancos de dados).

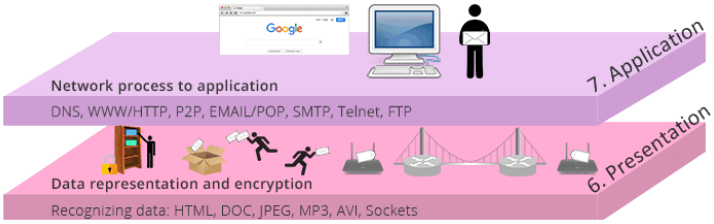


Nós dissemos anteriormente que o modelo divide a complexidade da comunicação em diversas camadas. Então vamos voltar para a nossa historinha de páginas atrás e consolidar tudo que vimos! A pergunta inicial era: *como um e-mail enviado para um amigo que mora do outro lado do mundo consegue chegar até o computador dele?* Bem, no momento que um amigo clica no botão de enviar e-mail para seu outro amigo, inicia-se um complexo fluxo de dados.

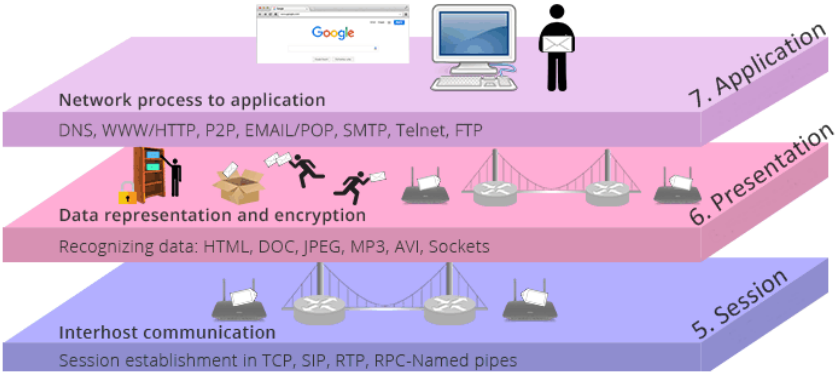
A primeira camada a receber o comando é a camada de aplicação. **Essa é a camada que serve como uma janela ou um portal para usuários ou processos acessarem serviços de rede.** *Como assim, professor?* Vejam só: se você deseja acessar uma página web, você pode usar o protocolo HTTP; se você deseja transferir um arquivo, você pode usar o protocolo FTP; e se você deseja enviar um e-mail, você pode usar o protocolo SMTP (esse é o nosso caso!).



Feito isso, os dados passam para a camada de apresentação, que será responsável por reconhecer o formato dos dados (verificar se se trata de uma mensagem, uma página web, uma foto, uma música, etc) e formatá-los, como uma espécie tradutor. **Na prática, ela traduz a mensagem escrita no alfabeto latino para uma linguagem que a máquina reconhece**. Além disso, ele poderá encriptá-la para que ninguém a intercepte e a leia durante o caminho.

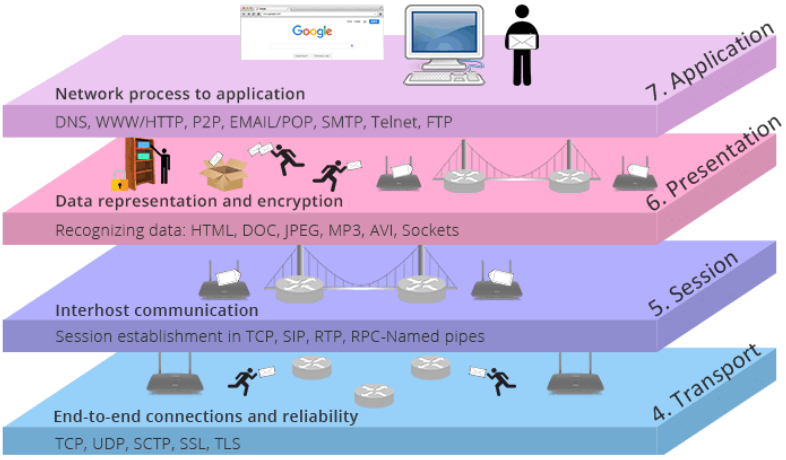


A partir daí, passamos para a camada de sessão, em que será estabelecida uma conexão entre a máquina de origem e a máquina de destino que permitirá que nós troquemos mensagens entre si. A Camada de Sessão também será responsável guardar várias informações relevantes para a comunicação (*Logging*).



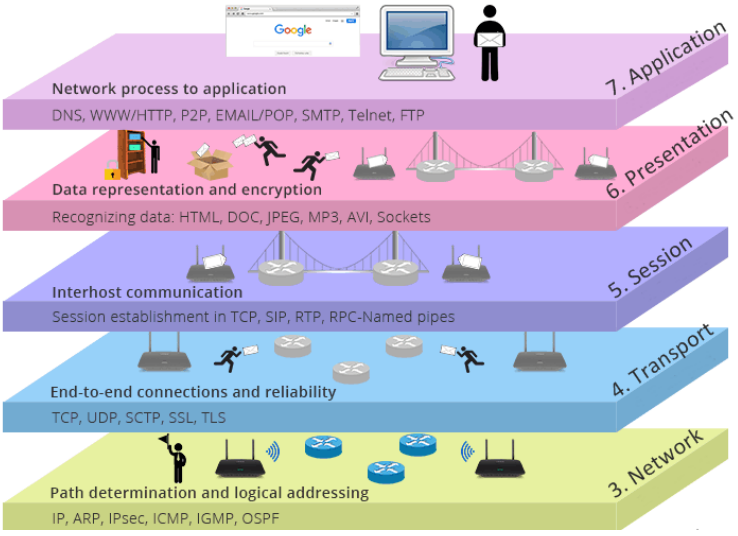
Beleza! Agora que minha informação acessou um serviço de rede que foi reconhecido na camada de apresentação e traduzido, formatado, encriptado e passado para a camada de sessão abrir uma conexão entre minha máquina e a máquina destino, **eu tenho que passar por uma camada que cuide da segurança e da validação da entrega dos dados**. *Pessoal,*

adianta alguma coisa se eu perder metade dos dados no caminho? Não, porque meu amigo não vai entender a mensagem.



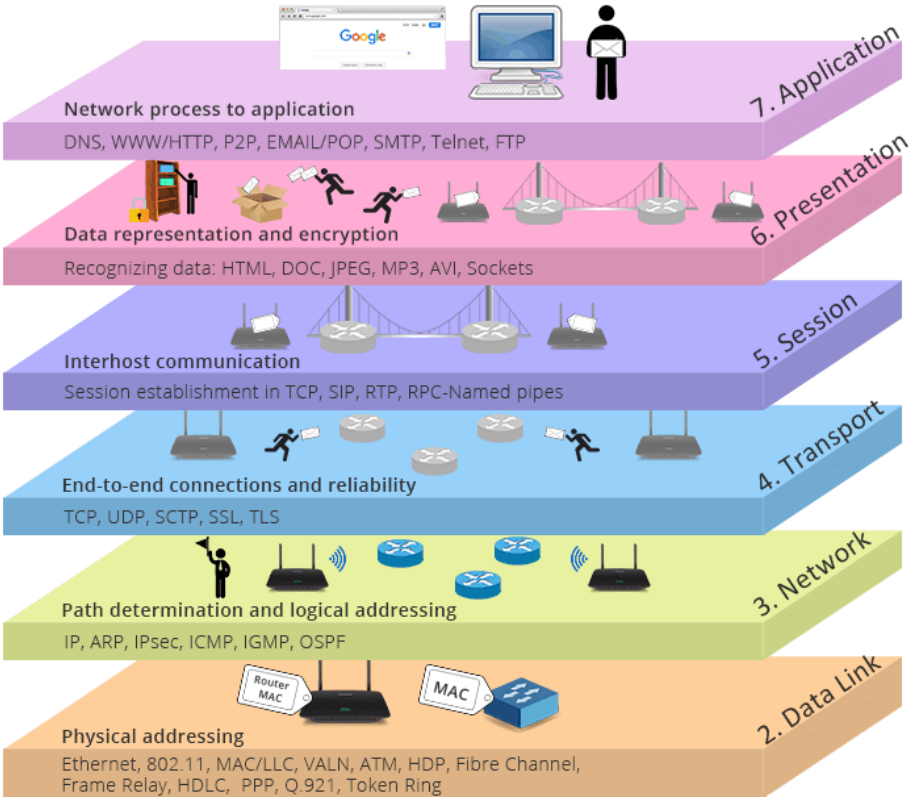
Adianta eu enviar todos os dados, mas em uma ordem toda bagunçada? Também não, ele continuará sem entender nada da minha mensagem. **A responsável por fazer uma varredura e garantir que o dado é confiável, íntegro e válido é a Camada de Transporte.** Além disso, notem uma coisa: nós não estamos mais era dos disquetes que cabiam 80kB! Hoje em dia, você pode enviar arquivos enormes por e-mail, por exemplo.

A rede não suporta dados tão grandes de uma vez, **logo é necessário dividi-los em pequenos segmentos**. Dados com problema serão destruídos e retransmitidos pela camada de transporte.

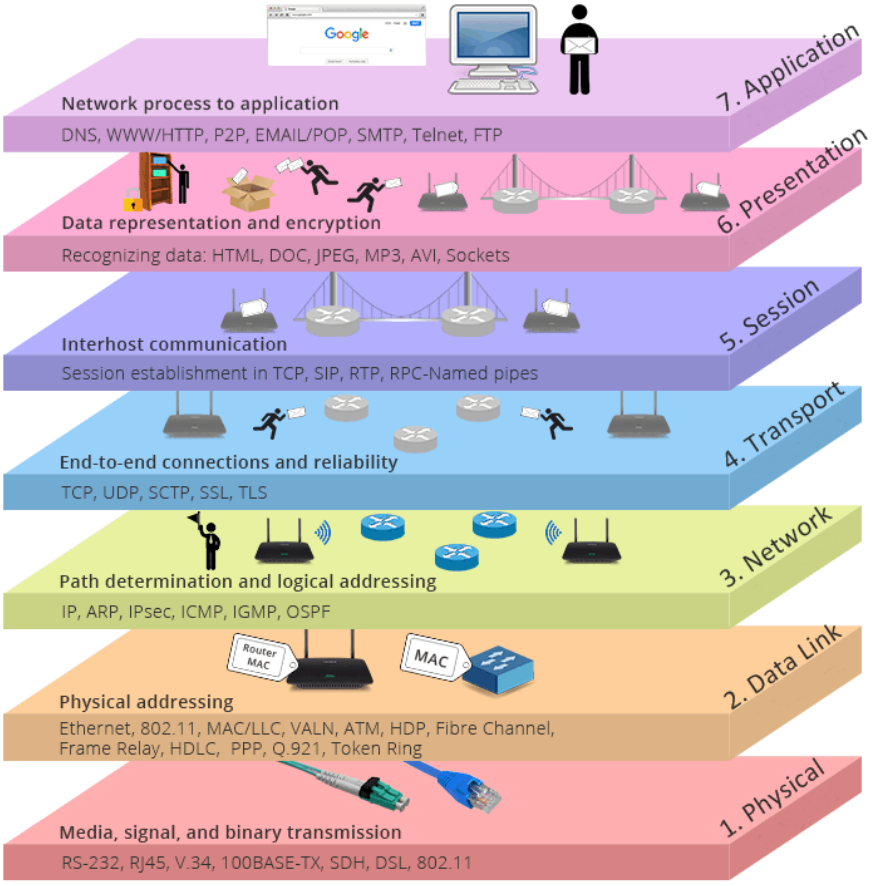


Passamos, então, para a famosa camada de redes (importantíssima em prova – falaremos em detalhes sobre seus protocolos em um tópico específico mais à frente)! **Aqui os segmentos serão encapsulados dentro de pacotes, que conterão o endereço lógico de origem e o endereço lógico de destino (também chamado de Endereço IP)**. Essa camada também vai determinar a rota que será utilizada baseado nas condições atuais da rede e na prioridade de entrega, isto é, cada nó intermediário do caminho. *Entendido?*

Em seguida, passamos para a Camada de Enlace, em que os pacotes são transformados em *frames* ou quadros para redes específicas. **Ela estabelece também uma conexão entre dois nós adjacentes sobre a Camada Física, permitindo uma comunicação virtualmente livre de erros entre esses nós.** Além disso, ele adiciona o endereço físico do nó de origem e do nó de destino (Endereço MAC). Vejamos:



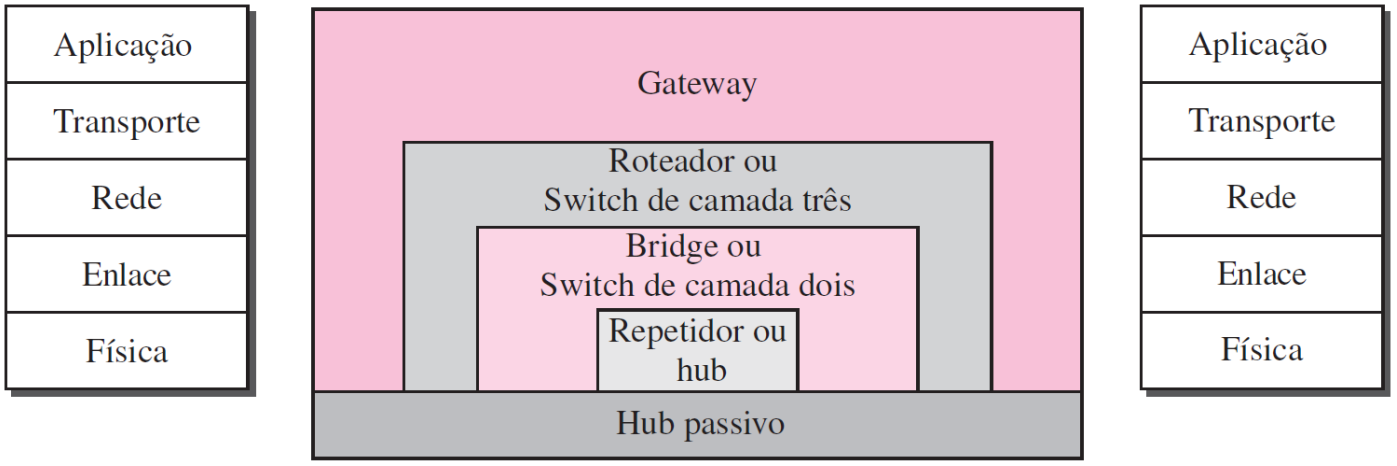
Por fim, chegamos à Camada Física, que transforma os frames em bits e finalmente os envia para a rede. Pode ser por meio daquele cabinho azul do computador, wi-fi, rádio, entre outros.

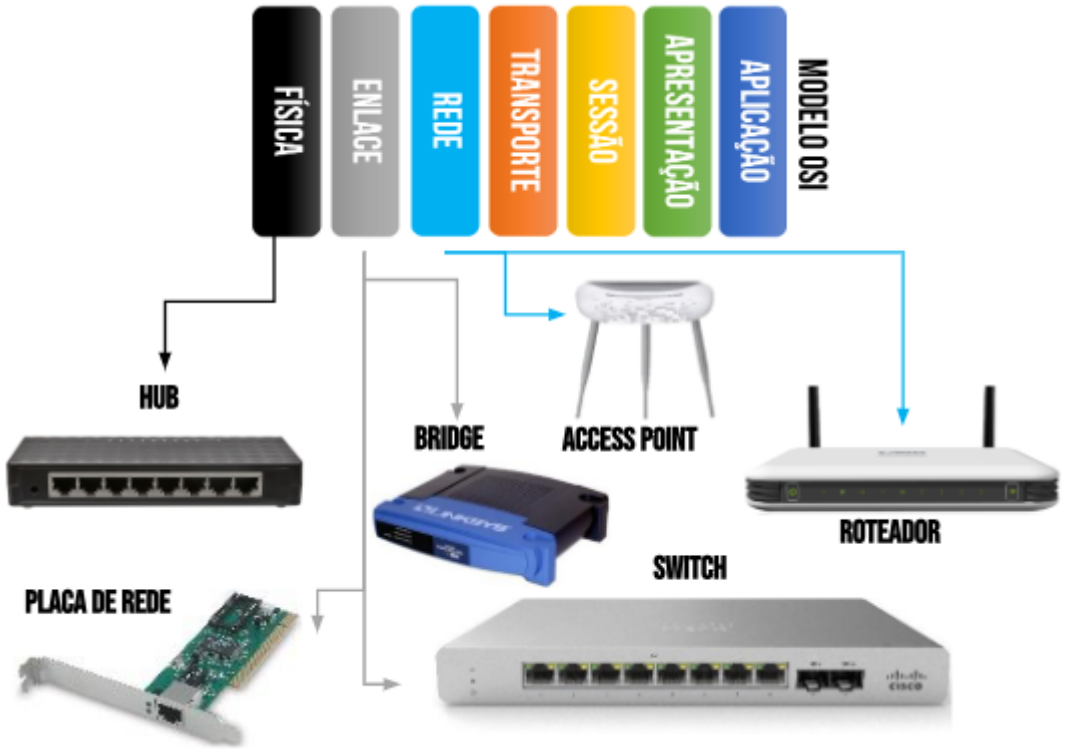


A partir daí, ficou fácil! Se for em uma rede cabeada, os bits passam da placa de rede do seu computador para o cabo azul, que passa para o seu roteador, que passa para o provedor de internet, que passa para o seu provedor de e-mail, que passa para o provedor de e-mail do seu amigo que passa para o roteador dele, que passa para o cabo azul dele, que passa para a placa de rede dele... Ufa! *Cansaram?*

E, finalmente, nós começamos todo esse processo, porém agora de forma invertida: iniciando na camada física da máquina de destino até chegar à camada de aplicação e o seu amigo clicar para ler o e-mail que você enviou. *Eu falei que ia ser legal, não falei?* Galera, claro que eu fiz algumas simplificações nessa explicação, mas não se preocupem porque alguns desses detalhes não serão tema de prova.

Por fim, nós vimos na aula anterior os principais dispositivos de rede. **Agora vejam na imagem em que camada trabalha cada um desses dispositivos**. É importante notar que cada dispositivo trabalha em uma camada principal, mas todos trabalham nas camadas abaixo de sua principal. Em outras palavras, as camadas são acumulativas – um roteador trabalha com foco na camada de rede, mas também trabalha – em algum nível – nas camadas física e de enlace.





#VamosPraticar#

(QUADRIX / CRECI11 – 2022) Para filtrar e encaminhar pacotes de dados, um switch utiliza as informações correspondentes à camada 2 do modelo OSI.

Comentários: um switch opera na camada de enlace (camada 2) do modelo OSI. Ele utiliza informações, como os endereços MAC (endereços de hardware) dos dispositivos na rede, para filtrar e encaminhar pacotes de dados (Correto).

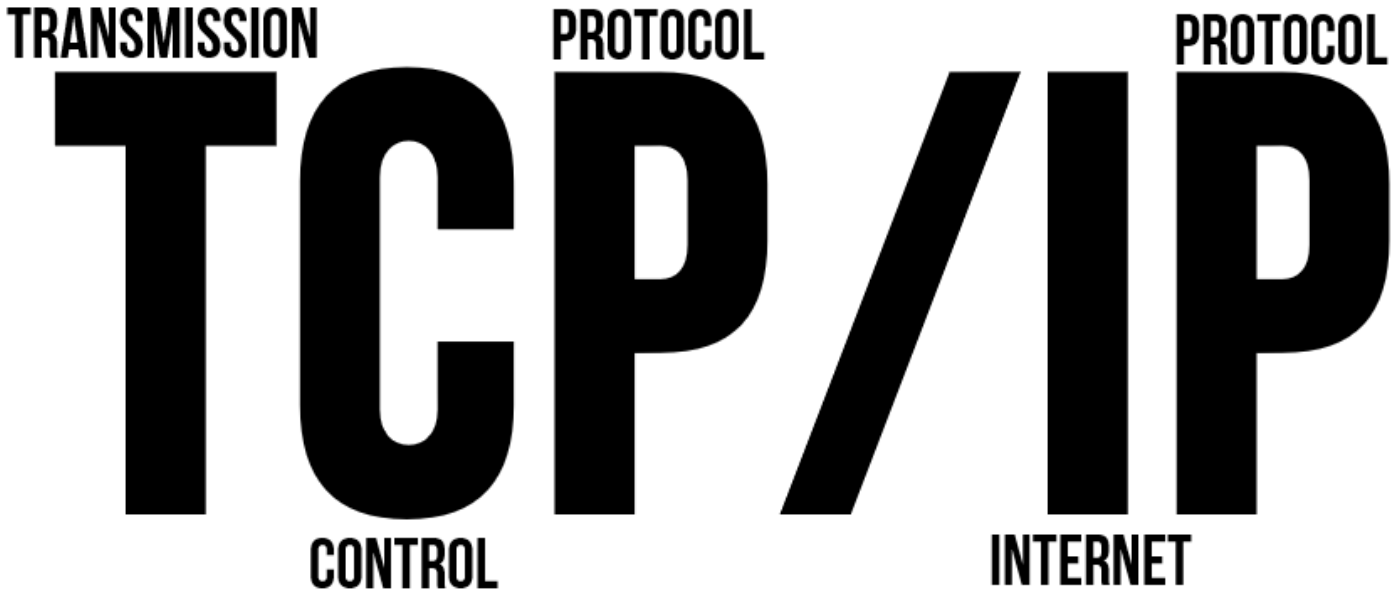
#VamosPraticar#

Redes de Computadores - Parte 2 - Arquitetura TCP-IP - Teoria

Arquitetura TCP/IP

INCIDÊNCIA EM PROVA: ALTA

ARQUITETURA TCP/IP
A arquitetura TCP/IP (*Transmission Control Protocol / Internet Protocol*) é um conjunto de protocolos de comunicação que são amplamente utilizados na internet e em redes locais. Ela fornece um conjunto de regras e especificações que permitem que diferentes dispositivos se comuniquem em redes de computadores, independentemente do fabricante ou sistema operacional.

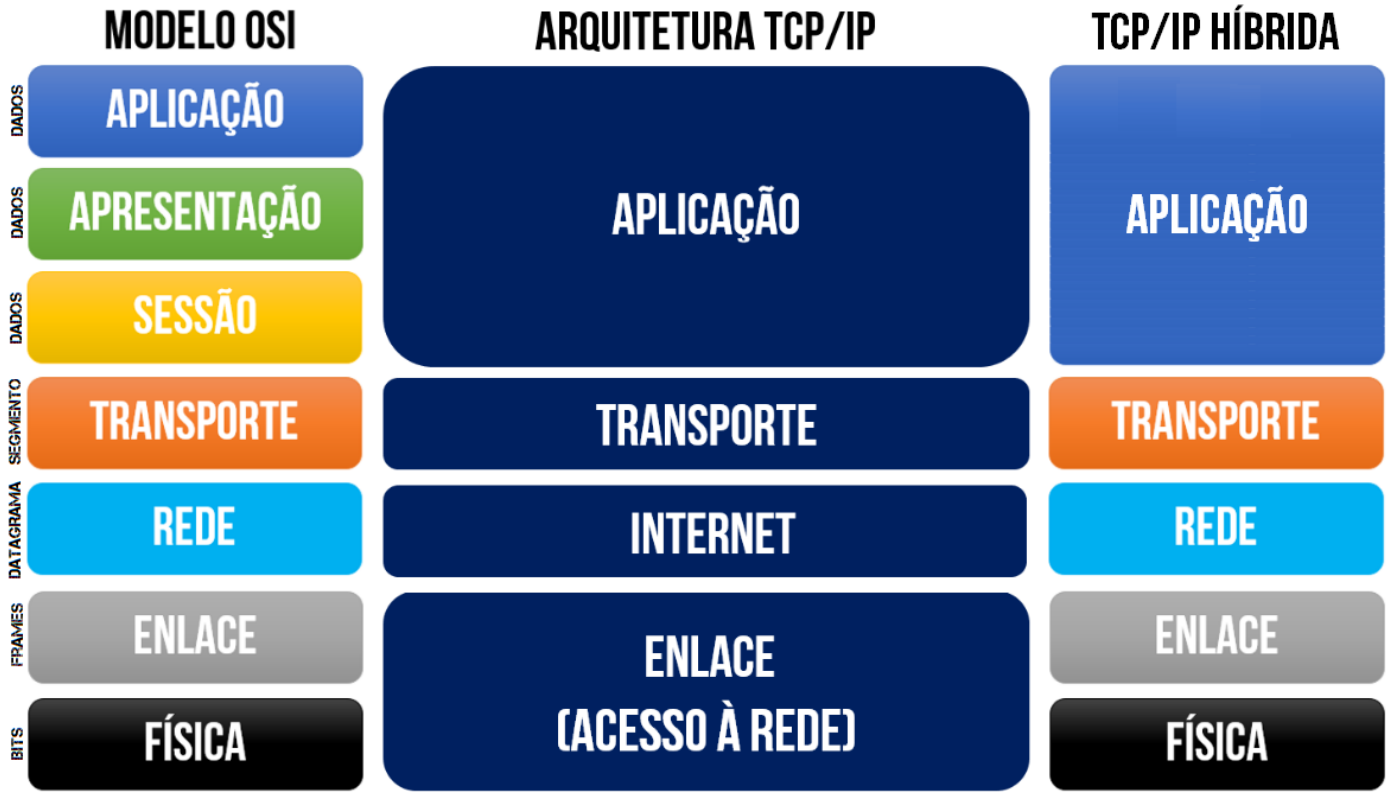


Nós acabamos de ver em detalhes o Modelo OSI e descobrimos que – apesar de ser um modelo conceitual bastante interessante e de facilitar o entendimento da comunicação entre redes – ele é apenas um modelo teórico utilizado didaticamente para mostrar o funcionamento ideal da comunicação de dados em uma rede de computadores. **Ele não é uma tecnologia, nem um conjunto de protocolos, nem um software e só tem utilidade pedagógica.**

Na prática, o que é utilizado é a Arquitetura ou Pilha TCP/IP. Essa arquitetura foi desenvolvida – na verdade – antes do Modelo OSI. Dessa forma, as camadas que nós veremos a seguir não correspondem exatamente àquelas do Modelo OSI. A Arquitetura TCP/IP é o conjunto de protocolos e camadas utilizados para conectar várias redes diferentes de maneira uniforme – **trata-se do conjunto padrão de protocolos da Internet.**

A quantidade e nome das camadas apresentada acima para a Arquitetura TCP/IP foi baseada na documentação oficial (RFC 1122). No entanto, alguns autores modelam essa arquitetura com três, quatro ou cinco camadas de nomes bastante diversos. Observem que ela condensa as camadas de aplicação, apresentação e sessão na camada de aplicação. Ademais,

ela condensa a camada física e de enlace na camada de enlace e chama a camada de rede de internet.



Eventualmente, quando um servidor – uma máquina especializada – fornece os serviços de um protocolo, é comum chamar esse servidor pelo nome do protocolo que ele implementa. Isso facilita a compreensão e a identificação de servidores e seus propósitos. Logo, temos que:

- **Servidor** que fornece serviços de páginas web pode ser chamado de **Servidor** HTTP;
- **Servidor** que fornece serviços de envio de e-mails pode ser chamado de **Servidor** SMTP;
- **Servidor** que fornece serviços de tradução de domínios pode ser chamado de **Servidor** DNS;
- **Servidor** que fornece serviços de transferência de arquivos pode ser chamado de **Servidor** FTP.

#VamosPraticar#

(CESPE / TELEBRÁS – 2022) O conjunto de protocolos TCP/IP, também conhecidos como protocolos de Internet, são os principais responsáveis pelo envio e recebimento de dados na comunicação dos computadores na Internet.

Comentários: o conjunto de protocolos TCP/IP é fundamental para a comunicação na Internet, sendo responsável pelo envio e recebimento de dados entre computadores na rede. Esses protocolos desempenham um papel essencial na transmissão de informações e na garantia de que os dados sejam entregues com sucesso, proporcionando a base para o funcionamento da Internet. Logo, o conjunto de protocolos TCP/IP é fundamental para a comunicação na Internet (Correto).

#VamosPraticar#

Redes de Computadores - Parte 2 - Principais Protocolos - Teoria

Principais Protocolos

Protocolos da Camada de Rede

IP (Internet Protocol)

INCIDÊNCIA EM PROVA: ALTÍSSIMA

INTERNET PROTOCOL (IP)

O IP é a base da comunicação na Internet, sendo responsável por rotear pacotes de dados de origem para destino em uma rede. Cada dispositivo conectado à Internet recebe um endereço IP exclusivo, que é usado para identificar e encaminhar dados para o destinatário correto. Quando um dispositivo deseja enviar dados para outro, ele divide os dados em pacotes. Cada pacote contém informações sobre o remetente, destinatário, dados reais e outros metadados – esses pacotes são então enviados pela rede. O roteamento é o processo pelo qual os pacotes são direcionados do remetente para o destinatário através de vários dispositivos intermediários, como roteadores.

O que significa essa sigla? Essa sigla significa **Internet Protocol**(em português, Protocolo de Internet).*Vamos traduzir também Internet?***Inter** significa *entre* e **net** significa *rede*, logo Internet significa *entre redes*. Agora vamos juntar tudo isso e dar um significado! IP é um protocolo – um conjunto de normas, padrões e convenções – para comunicação entre redes. **O endereço IP define de forma única e universal a conexão de um dispositivo** (Ex: um computador ou um roteador).

#VamosPraticar#

(CESGRANRIO / BB – 2023) A rede global de computadores, conhecida como internet, foi difundida ao longo dos últimos anos entre vários países ao redor do mundo e revolucionou a forma como as pessoas vivem. A internet é formada por redes de comunicação de dados interligadas globalmente que trocam dados entre si, utilizando um protocolo de comunicação comum chamado:

a) Earth Protocol (EP)

b) World Protocol (WP)

c) Global Protocol (GP)

d) Internet Protocol (IP)

e) Neutral Protocol (NP)

Comentários: a internet é uma rede global de computadores interconectados, e o protocolo de comunicação comum que permite a troca de dados entre esses computadores é chamado de Internet Protocol (IP). O IP é essencial para a comunicação e roteamento de dados na internet. As outras alternativas, como Earth Protocol (EP), World Protocol (WP), Global Protocol (GP) e Neutral Protocol (NP), não representam protocolos de comunicação comumente utilizados na internet (Letra D).

#VamosPraticar#

Eles são exclusivos no sentido de que cada endereço define uma única conexão com a Internet – dois dispositivos jamais podem ter o mesmo endereço ao mesmo tempo na mesma rede. Além disso, eles são universais no sentido de que o sistema de endereçamento

tem de ser aceito por qualquer host (máquina) que queira se conectar à Internet. Agora vamos ver uma analogia para entender o seu funcionamento...

IP: Funcionamento

Imagine que você queira enviar uma carta para um amigo que mora em uma outra cidade. Essa carta é como um pacote de dados na Internet. Vamos comparar cada elemento:

- Passo 1: Endereço do Destinatário (Endereço IP)

+	0 - 3	4 - 7	8 - 15	16 - 18	19 - 31
0	Versão	Tamanho do cabeçalho	*Tipo de Serviço* (ToS) (agora DiffServ e ECN)	Comprimento (pacote)	
32	Identificador			*Flags*	*Offset*
64	*Tempo de Vida* (TTL)		Protocolo	*Checksum*	
96	Endereço origem				
128	Endereço destino				
160	Opções				
192	*Dados*				

Antigamente, para enviar uma carta a alguém, você pegava um pedaço de papel, escrevia diversas informações, colocava dentro de um envelope com o endereço de origem (remetente) e endereço de destino (destinatário). Na internet, ocorre de maneira bastante similar: as informações que eu desejo transmitir são encapsuladas dentro de um envelope chamado Pacote IP, que contém necessariamente um endereço IP de origem e um endereço IP de destino. **Na Internet, cada dispositivo possui um endereço IP exclusivo.**

A imagem anterior apresenta o formato de um Pacote IP (Versão 4). Notem que existem diversos campos, mas aqui vamos nos focar em apenas quatro:

CAMPOS do ip	DESCRIÇÃO
VERSÃO	Trata-se da versão do IP (IP Versão 4 ou IP Versão 6);
ENDEREÇO DE ORIGEM	Trata-se do IP do Remetente;
ENDEREÇO DE DESTINO	Trata-se do IP do Destinatário;
DADOS	Trata-se da carga útil de dados que serão enviados.

O Protocolo IP é responsável por especificar o formato desse Pacote IP que trafegará entre roteadores e sistemas finais. Voltando à nossa analogia: assim como no Pacote IP, um envelope pode conter outras informações além dos dados em si (Ex: carimbo de identificação, data de envio da carta, quantidade de palavras contidas, entre outros). Em outras palavras, o Pacote IP conterá os dados em si, além de um cabeçalho com diversas outras informações que facilitem a entrega.

- Passo 2: Divisão em Pacotes

Agora uma pergunta: *eu posso enviar um processo com 50.000 páginas pelos Correios?* Posso! No entanto, os Correios não vão conseguir colocar 50.000 páginas dentro de um único envelope!

Os Correios impõem um tamanho limite para o pacote que ele é capaz de transportar, da mesma forma que existe um tamanho limite para o pacote IP. *E qual é o tamanho, Diego?* **Esse limite é de 64 Kb!** *Caraca, professor... por que tão pequeno?* Galera, quando a internet foi criada, isso era uma quantidade absurda de informação. Vejam essa imagem ao lado: isso é um HD de 1960 capaz de armazenar estrondosos 5 Mb de informação. *Incrível, não?* Claro que não é mais assim hoje em dia. Uma foto tirada pelo celular possui cerca de 6.4 Mb (= 6400 Kb). *E se eu quiser enviar essa foto para outra pessoa, caberá tudo em um pacote?* Jamais! **O IP terá que dividir a foto em pacotes de 64 Kb**. Como 6400 Kb dividido por 64 Kb é 100, teremos que dividir a foto em 100 pacotinhos e enviá-los um a um.

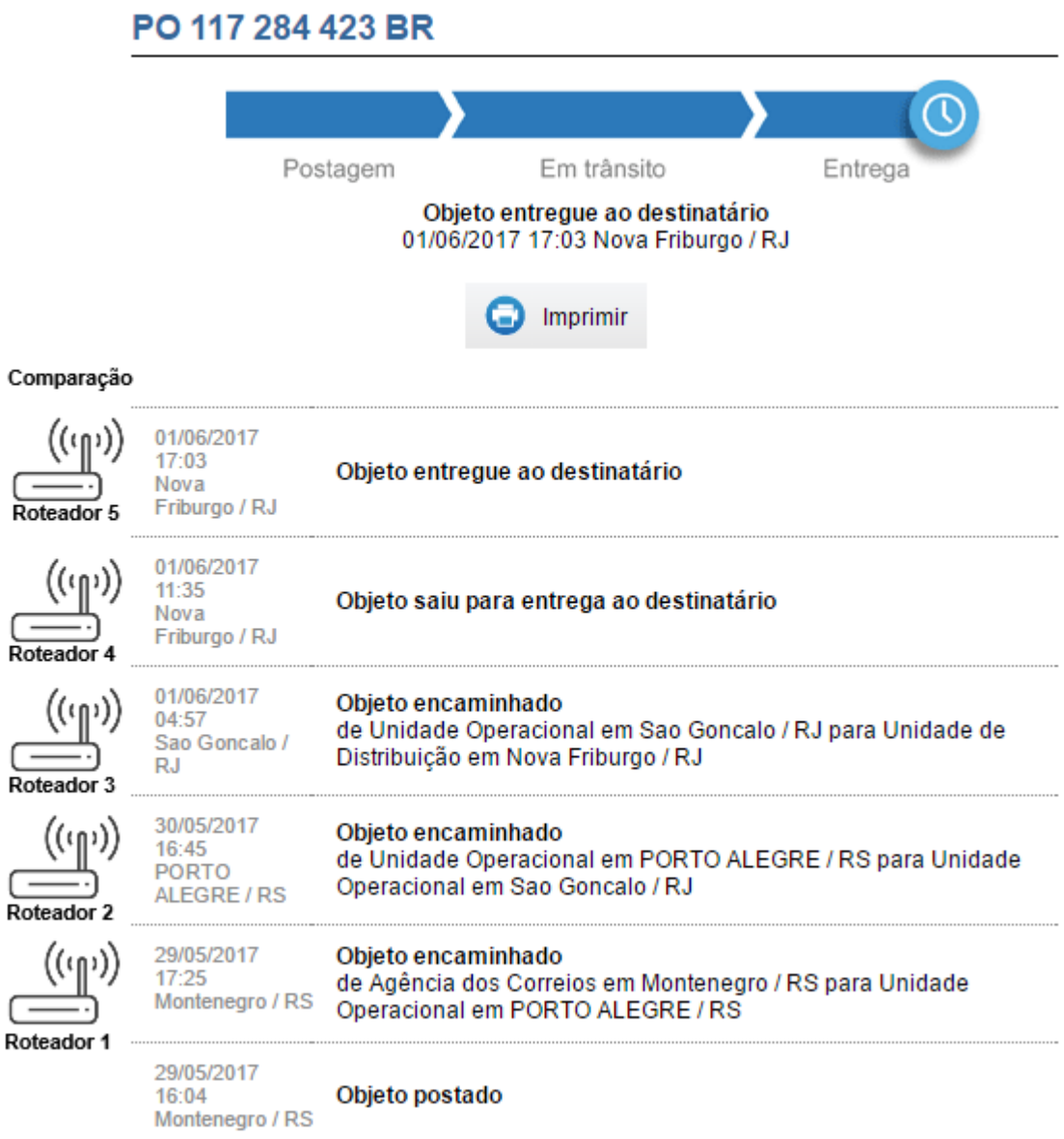
Em suma: o IP divide dados grandes em pacotes menores antes de enviá-los pela rede em um processo conhecido como **Fragmentação de Pacotes**. Ele ocorre quando um pacote é muito grande para ser transmitido em uma rede com uma determinada capacidade máxima de carga útil. Quando um roteador encontra um pacote que é maior do que o tamanho máximo permitido pela rede seguinte (MTU - *Maximum Transmission Unit*), ele divide o pacote em fragmentos menores.

Cada fragmento contém uma parte dos dados originais e é transmitido separadamente pela rede. No destino, os fragmentos são reagrupados para recriar o pacote original.

Para ouvir ao áudio correspondente, acesse o LDI.

- Passo 3: Correios (Roteadores)

Agora que você já fragmentou sua encomenda em envelopes menores, você poderá entregá-los em uma agência dos correios local. Essa agência é como o roteador mais próximo. *Sabe quando você vai rastrear um pacote dos correios em que ele mostra cada agência que o pacote passou até chegar à sua casa?* Pois é, os correios são os responsáveis por encaminhar cada envelope para a agência de destino. **Os roteadores fazem o mesmo, encaminhando pacotes pela rede.**



- Passo 4: Roteamento

O roteamento refere-se ao processo de encaminhar pacotes de dados de um dispositivo de origem para um dispositivo de destino através de uma rede. Envolve a escolha do caminho mais eficiente e adequado entre os diversos dispositivos interconectados na rede, assim como cada agência dos correios sabe como chegar a outras agências. Eles decidem para onde encaminhar cada envelope com base no endereço do destinatário.

O dispositivo de origem envia o pacote para o roteador mais próximo. O roteador consulta sua tabela de roteamento para determinar para onde encaminhar o pacote. Com base nas informações da tabela de roteamento, o roteador decide qual é o próximo dispositivo (roteador) ao longo do caminho até o destino. **Essa escolha é feita com base no endereço IP de destino e nas informações de roteamento.**

O roteador encaminha o pacote para o próximo dispositivo ao longo do caminho. Esse processo se repete em cada roteador ao longo do percurso até o pacote atingir seu destino final. Os roteadores utilizam métricas (como distância, largura de banda, atraso) para determinar a

melhor rota para um pacote, escolhendo caminhos eficientes com base nas condições da rede. **Da mesma forma, os Correios utilizam métricas para determinar a melhor rota de entrega de um pacote.**

#VamosPraticar#

(QUADRIX / CRB9 – 2023) O IP (Internet Protocol) é um sistema de roteamento cuja função é a determinação da melhor rota para os pacotes de dados em uma rede.

Comentários: IP é um protocolo que fornece um endereço lógico para dispositivos conectados à internet e, não, um sistema de roteamento. O responsável por determinar a melhor rota para os pacotes de dados em uma rede é o roteador (Errado).

#VamosPraticar#

- Passo 5: Entrega ao Destinatário

Finalmente, os envelopes chegam à agência dos correios mais próxima do seu amigo, que os encaminha até a casa dele. Já os roteadores garantem que pacotes cheguem ao destino final.

- Passo 6: Montagem de Pacotes

Seu amigo recebe os envelopes e os reúne para reconstruir a carta original. Dispositivos no destino fazem algo semelhante, montando os pacotes para obter os dados originais.

IP: Características

O IP possui duas características importantes que podem cair em prova. Trata-se de um protocolo de distribuição de pacotes **não confiável** (ou de melhor esforço) e **sem conexão**. Vejamos:

a) Não confiável

O IP é considerado um protocolo de comunicação "não confiável" porque não fornece garantias de entrega de dados, confirmação de recebimento ou controle de fluxo. **Ele é projetado para fornecer roteamento eficiente de pacotes de dados pela rede, mas não inclui mecanismos embutidos para verificar se os pacotes realmente chegam ao destino.** Vejamos algumas razões pelas quais esse protocolo é considerado não confiável:

Características do ip	DESCRIÇÃO

Sem confirmação de entrega	IP não possui um mecanismo integrado para confirmar se um pacote de dados chegou ao destino. Após enviar um pacote, não há garantia de que ele será recebido com sucesso.
Sem controle de fluxo	IP não gerencia o controle de fluxo, o que significa que não ajusta automaticamente a taxa de transmissão de dados com base na capacidade da rede ou na capacidade de processamento do destinatário. Isso pode levar a congestionamentos e perda de pacotes.
Sem reordenação de pacotes	IP não reordena automaticamente pacotes fora de ordem. Se os pacotes forem recebidos fora de sequência, cabe às camadas superiores, como o protocolo de transporte (como TCP), lidar com a reordenação.
Sem garantia de integridade	IP não verifica a integridade dos dados dentro dos pacotes. Se houver corrupção nos dados durante a transmissão, o IP não detectará ou corrigirá automaticamente.

Galera, por que dizemos que o IP é um protocolo de melhor esforço (best-effort)? Porque – por mais que ele se esforce –, ele não é capaz de **garantir** que a entrega será realizada. Sabe o motorista do caminhão dos Correios? Ele geralmente é um cara experiente que já dirigiu pelo Brasil inteiro e conhece as melhores rodovias e rotas para realizar suas entregas sem nem precisar acessar o Waze. Ele fará tudo que estiver em seu alcance para realizar a entrega, mas ele não pode garantir nada.

O que ele pode fazer se houver um acidente na estrada? Se estiver tudo engarrafado? Se ocorrer uma nova greve dos caminhoneiros? Ele pode tentar utilizar outra rota, mas a entrega dos pacotes certamente atrasará. Pior: *e se infelizmente ele for assaltado no meio do caminho e os ladrões levarem parte da carga de seu caminhão?* Ele perderá pacotes e não conseguirá realizar a entrega.

Por essa razão, dizemos que o Protocolo IP é não confiável (ou de melhor esforço). *Professor, qual é a alternativa para solucionar esse problema?* Para fornecer confiabilidade na transmissão de dados, é comum usar protocolos de camada superior (Ex: TCP). Esse protocolo adiciona funcionalidades de confirmação de entrega, controle de fluxo, reordenação de pacotes e verificação de integridade, tornando a comunicação mais confiável. Veremos em detalhes mais à frente...

b) Sem Conexão

O IP é considerado um protocolo "sem conexão" porque não estabelece uma conexão prévia antes de enviar dados. **Em vez disso, cada pacote de dados contém dados suficientes para serem tratados independentemente e roteados separadamente pelos dispositivos de rede.** Dessa forma, eles podem seguir caminhos diferentes pela rede e chegar ao destino em ordens diferentes daquela em que foram enviados.

IP: Classificação

Endereços IP podem ser classificados em estáticos ou dinâmicos. Essa classificação trata de como os endereços IP são atribuídos aos dispositivos em uma rede de computadores. A escolha entre endereços IP estáticos e dinâmicos depende dos requisitos específicos da rede, da escala da infraestrutura e das necessidades de gestão dos endereços. Muitas redes utilizam uma combinação de ambos para atender às diversas demandas. Vejamos...

a) IP Estático

Também chamado de IP Fixo, são atribuídos manualmente aos dispositivos e permanecem constantes, não mudando automaticamente. A sua configuração geralmente é feita manualmente pelo administrador da rede. Isso pode ser feito no dispositivo em si ou por meio de configurações no servidor DHCP (veremos mais à frente). Sua utilização é mais comum quando um dispositivo precisa ter sempre o mesmo endereço (Ex: servidores, impressoras e roteadores).
As principais vantagens desse tipo de Endereço IP é a facilidade da administração, dado que os endereços são previsíveis e conhecidos. **Além disso, conforme já vimos, pode ser útil para dispositivos que precisam ser sempre acessíveis com o mesmo endereço.***Sabe quem tem um IP Estático?* O servidor web do Estratégia Concursos! Toda vez que você acessa a página do Estratégia, ela acessa o mesmo servidor web que possui sempre o mesmo Endereço IP.

b) IP Dinâmico

São atribuídos automaticamente por um servidor DHCP na rede sempre quando um dispositivo se conecta. Os dispositivos obtêm um endereço temporário que precisa ser renovado periodicamente e o servidor DHCP gerencia esse processo de renovação. Os endereços IP dinâmicos são alocados conforme necessário, evitando a necessidade de atribuir manualmente endereços e permitindo um uso mais eficiente do espaço de endereço.

Em suma, os dispositivos podem receber endereços IP diferentes em cada conexão, dependendo do pool de endereços disponíveis no servidor DHCP. **Ele facilita a gestão em redes grandes, pois não é necessário atribuir manualmente endereços a cada dispositivo.** Além disso, aumenta a eficiência na utilização do espaço de endereçamento. *Sabe quem tem um IP Dinâmico?* Eu (e muito provavelmente você).

Pois é... cada vez que eu me conecto à internet, é atribuído um novo endereço IP a minha máquina. O IP Dinâmico é bem mais utilizado que o IP Estático, principalmente em redes

domésticas.

IP: Versionamento

Agora vamos falar um pouquinho sobre versões do Protocolo IP. Nós temos basicamente duas versões: **IPv4** (Versão 4) e **IPv6** (Versão 6). Vamos iniciar nosso papo falando sobre o IPv4!

a) IPv4 (Versão 4)

Esse protocolo utiliza endereços de 32 bits, que podem ser representados por meio de duas notações: **Notação de Octetos Binários**ou **Notação Decimal Pontuada**. Ambas as notações são comumente utilizadas, mas a Notação Decimal Pontuada é mais intuitiva para os humanos, facilitando a leitura e compreensão dos endereços IP. No entanto, antes de prosseguir, vamos falar um pouco sobre numeração...

Existem diversos sistemas de numeração! Seres humanos utilizam um sistema de numeração decimal, isto é, nós fazemos contas utilizando dez dígitos (0, 1, 2, 3, 4, 5, 6, 7, 8 e 9). Já os computadores utilizam um sistema de numeração binária, isto é, eles fazem contas utilizando apenas dois dígitos (0 e 1) – o nome desse dígito binário é Bit (do inglês, Binary Digit). É possível converter números de um sistema para outro sem nenhum inconveniente. Vejam abaixo o número 123 em outros sistemas numéricos:

SISTEMA DECIMAL	SISTEMA HEXADECIMAL	SISTEMA OCTAL	SISTEMA BINÁRIO
123	7B	173	01111011

Na notação de octetos binários, os 32 bits são representados por meio de quatro conjuntos de oito bits, sendo que esse conjunto de 8 bits (ou 1 byte) é chamado de octeto:

Endereço Ip com notação de octetos binários			
10101010	01010101	11100111	10111101

Ocorre que utilizar endereço em bits pode acabar incorrendo em erros. Como só temos os dígitos 0 e 1, se você tem miopia, pode acabar errando. **Por conta disso, alguém teve a brilhante ideia de converter esses números do sistema binário para o sistema decimal**. Dessa forma, cada octeto em binário pode ir de 0 a 255 em decimal (você nunca vai encontrar um número que esteja fora dessa extensão). Se convertermos os números da notação anterior para notação decimal, teremos:

Endereço IP com NOTAÇÃO DECIMAl pontuada						
170	.	85	.	231	.	189

#VamosPraticar#

(PC/SP – 2017)

Assinale a sequência numérica abaixo que pode representar o Endereço IP (Internet Protocol) válido de um microcomputador em uma rede:

a) 10.260.25.200

b) 10.35.29.129

c) 10.0.40.290

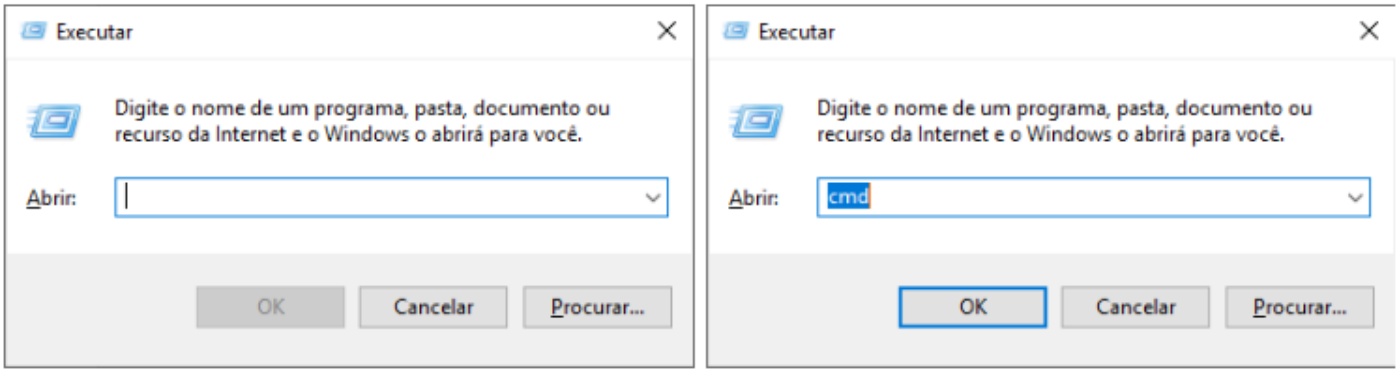
d) 10.0.290.129

e) 10.35.260.290

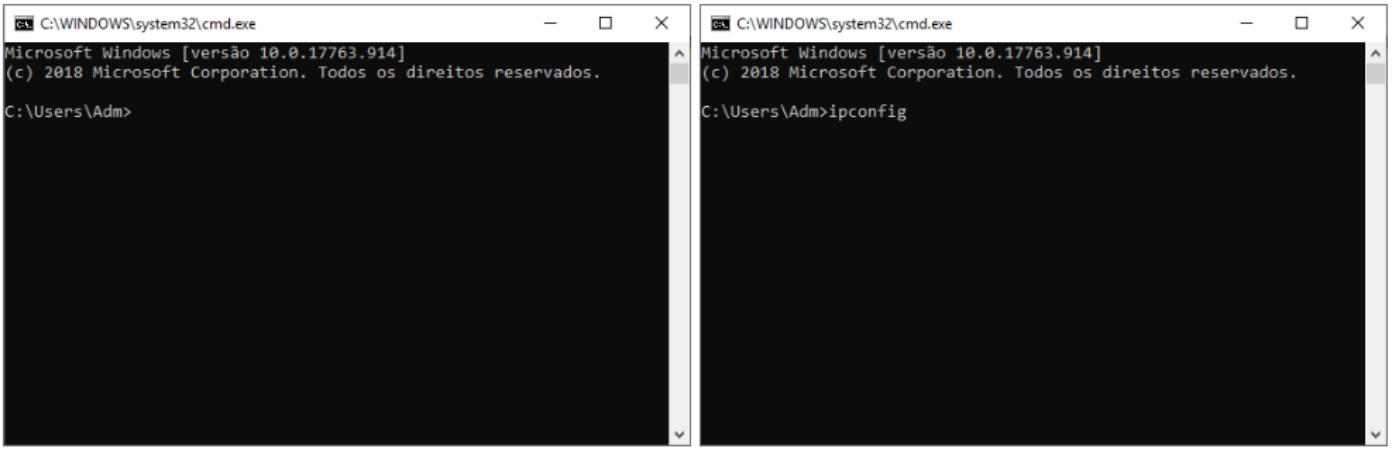
Comentários: Endereços IP válidos no padrão IPv4 são compostos por quatro partes numéricas separadas por pontos (por exemplo, 192.168.1.1), e cada parte deve estar dentro do intervalo de 0 a 255. Portanto, um endereço IP válido não pode ter partes numéricas maiores que 255.ele varia de 0 a 255. Com base nisso, nós podemos analisar: (a) Errado, 260 > 255; (b) Correto; (c) 290 > 255; (d) 290 > 255; (e) 260 e 290 > 255 (Letra B).

#VamosPraticar#

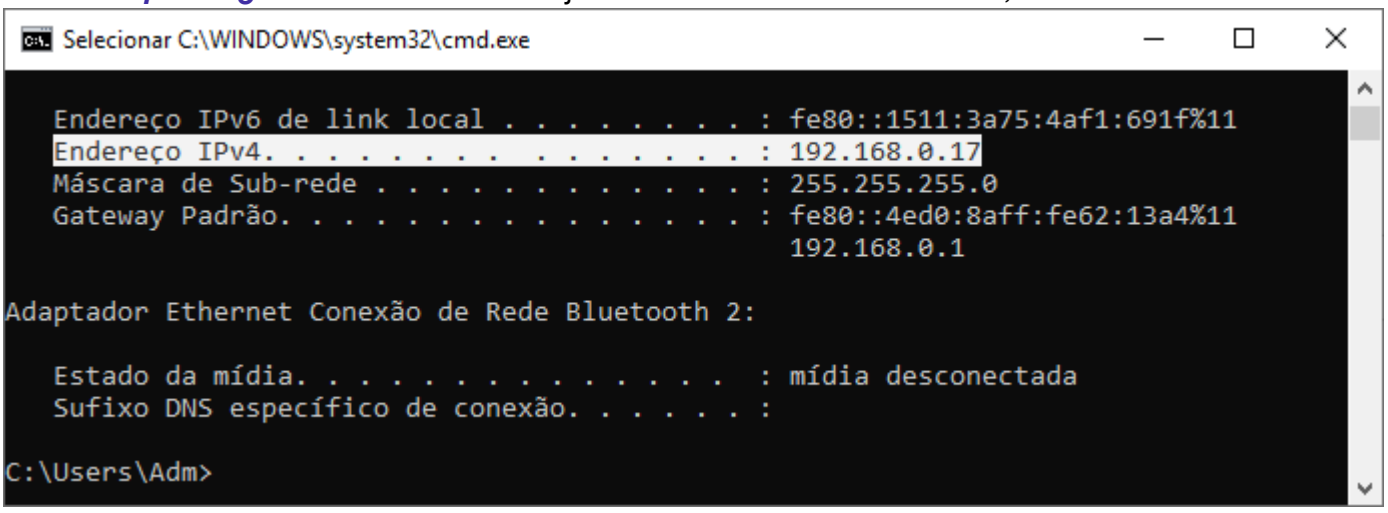
Professor, está tudo muito abstrato! Você pode dar um exemplo? Claro! Para tal, eu vou propor um exercício para vocês: eu quero que vocês pressionem simultaneamente as teclas Windows + R.



Quando vocês fizerem isso, aparecerá essa imagem da esquerda. Eu quero, então, que vocês escrevam o comando ***cmd*** conforme vemos na imagem da direita.



Notem que será exibida essa janela da esquerda. Em seguida, eu quero que vocês escrevam o comando ***ipconfig*** conforme vemos na janela da direita. No meu caso, foi exibido:



Eu destaquei em branco uma informação importante: meu Endereço IPv4 é **192.168.0.17**! Logo, se alguém quiser me encontrar nesse dia, esse era o endereço lógico do meu computador na Internet.

Pessoal, é importante entender que esses endereços que vimos anteriormente no IPv4 não são aleatórios: existem diversas regras que devem ser obedecidas para cada endereço. Uma delas é o **Endereçamento por Classes**. *O que é isso, Diego?* Trata-se de uma abordagem para a alocação de endereços IP e foram criadas para alocar blocos de endereços de maneira mais estruturada e eficiente.

Com o crescimento da internet, era necessário alocar blocos de endereços IP de acordo com o tamanho das redes. Redes maiores precisavam de mais endereços do que redes menores. Para atender a essa demanda por tamanhos variados de blocos de endereços, as classes foram introduzidas para estruturar e classificar os endereços IP em categorias que correspondessem ao tamanho das redes.

As classes permitiam identificar o tamanho aproximado da rede com base no endereço IP. Por exemplo, uma empresa que necessitasse de muitos endereços teria uma classe de endereço diferente de uma rede doméstica pequena. Galera, nós já sabemos que um endereço IPv4 possui 32 bits e já sabemos também que um bit só pode ter dois valores (0 ou 1). Logo, nós temos 2^{32} ou 4.294.967.296 endereços possíveis.
O endereçamento por classes busca dividir esse espaço de endereços possíveis em cinco classes: Classe A, Classe B, Classe C, Classe D e Classe E. Logo, todo e qualquer IP pode ser classificado em uma dessas cinco classes. *E como eu faço para descobrir à qual classe um endereço pertence, professor?* É extremamente simples: basta analisar o primeiro número (na notação decimal pontuada) conforme é apresentado na tabela seguinte:

1º octeto	CLASSE	UTILIZAÇÃO
0 A 127 [3]	A	Inicialmente destinado a grandes organizações.
128 A 191	B	Inicialmente destinado a organizações de médio porte.
192 A 223	C	Inicialmente destinado a pequenas organizações.
224 A 239	D	Inicialmente destinado a reservado para *multicast*.
240 A 255	E	Inicialmente destinado a reservado para testes.

Como interpreta essa tabela? É bem simples! Se o primeiro número de um endereço IP for de 1 a 126, ele será da Classe A (geralmente utilizado por grandes organizações); se for de 128 a 191, ele será da Classe B (geralmente utilizado por organizações de médio porte); se for e 192 a 223, ele será da Classe C (geralmente utilizado por pequenas organizações); se for de 224 a 239, será da Classe D (reservado para *multicast*); e se for de 240 a 255, será da Classe E (reservado para testes).

Nós vimos acima que existem quase 4.3 bilhões de possibilidades de Endereços IP, no entanto esse valor é bem menor na prática. Endereços de Classe D e Classe E não podem ser utilizados na internet. Além disso, vários endereços são proprietários ou reservados para alguma organização. *Vocês sabiam que a Apple é dona de todo IP que se inicia pelo número 17 e a Ford de todo IP que se inicia por 19?* **Pois é... apenas cerca de metade dos endereços podem realmente ser utilizados.**

Atualmente, a utilização das classes de endereçamento foi amplamente substituída por abordagens mais flexíveis, permitindo uma alocação mais precisa de endereços com base nas necessidades específicas das redes, resultando em uma gestão mais eficiente do espaço de endereço disponível. Agora eu preciso fazer uma pequena confissão para vocês: eu menti na página anterior! *Quando, Diego?* Quando eu mostrei o meu endereço na janelinha preta...

Aquele endereço não era meu endereço IPv4 real! *Como assim, professor?* **Pessoal, todo dispositivo em uma mesma rede necessita de um Endereço IP único – não podem existir dois dispositivos com o mesmo Endereço IP!** No entanto, com o passar dos anos a quantidade de dispositivos conectados à internet aumentou assustadoramente. Por exemplo: na minha casa, há dois smartphones, dois computadores, um notebook, dois tablets e dois smartwatches.

Só na minha casa há nove dispositivos conectados à internet. *E na casa do vizinho? E no condomínio? E no bairro? E na cidade? E no país? E no mundo?* Lembrando que o nosso planeta acabou de alcançar a marca de 8 bilhões de pessoas – quatro vezes a quantidade efetiva de endereços possíveis no IPv4 (e, como disse, nem todos estão disponíveis). **Logo, algo precisava ser feito antes que chegássemos ao total esgotamento de endereços.**

Nesse momento, os engenheiros tiveram que arrumar uma solução enquanto não havia uma nova versão para o Protocolo IP. *E como eles fizeram, Diego?* Eles resolveram de uma maneira genial! **Pensem comigo: uma coisa é a rede doméstica privada na sua casa/escritório e outra coisa é a rede mundial de computadores (Internet).** Logo, os engenheiros padronizaram algumas faixas de endereços que deveriam ser utilizados exclusivamente para redes privadas.

Professor, eles reduziram mais ainda a quantidade de endereços efetivamente possíveis na internet? Sim (parece contraditório, mas vocês vão entender). **Todo Endereço IP que estivesse dentro dessa faixa que eles convencionaram não poderiam ser utilizados na internet – eles só poderiam ser utilizados em redes internas.** *Que valores são esses?* Na tabela a seguir, nós podemos ver quais são essas faixas de endereços:

Classe	Faixa de Endereços para redes privadas
A	10.0.0.0 até 10.255.255.255
B	172.16.0.0 até 172.31.255.255
C	192.168.0.0 até 192.168.255.255

#VamosPraticar#

(CEFET / CEFET – 2021) Os endereços IP da faixa 192.168.255.0 - 192.168.255.255 são

a) de broadcast.

b) de multicast.

c) de classe A.

d) privados.

e) públicos.

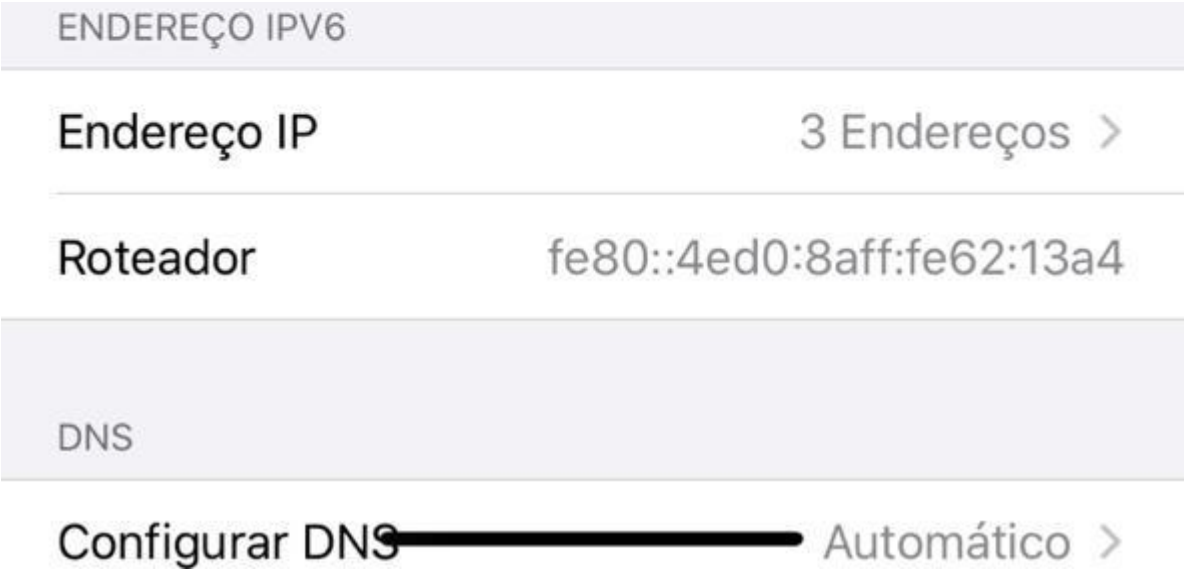
Comentários: a faixa de endereços IP 192.168.255.0 - 192.168.255.255 pertence a uma faixa de endereços IP privados. Esses endereços são reservados para uso em redes locais (LANs) e não são roteados na Internet pública. Essa faixa de endereços específica é uma parte da faixa maior de 192.168.0.0 - 192.168.255.255, que é designada para uso em redes privadas (Letra D).

#VamosPraticar#

Professor, ainda não entendi por que você disse que mentiu? Pessoal, eu disse algumas páginas

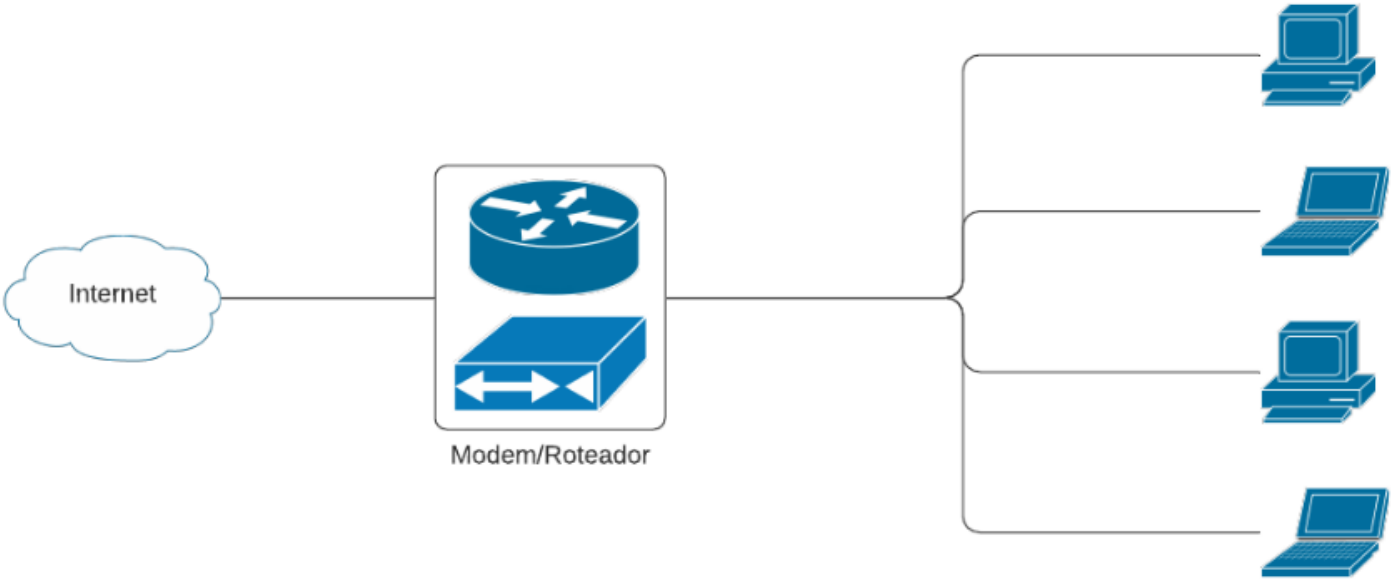
atrás que o meu IP era **192.168.0.17.** **Façam-me um favor: confiram agora na tabela apresentada se esse endereço informado está presente em alguma dessas faixas!** Ora, está dentro da Classe C! Logo, eu não menti exatamente para vocês – eu apenas informei qual era o meu endereço IP dentro da minha rede doméstica – também chamado de IP Privado ou Local!

05:36
Wi-Fi
KitDiego
Esquecer Esta Rede
Conexão Automática
Modo de Economia de Dados
O Modo de Economia de Dados ajuda os apps do iPhone a reduzir o uso de dados da rede.
ENDEREÇO IPV4
Configurar IP
Automático
Endereço IP
192.168.0.20
Máscara de Sub-rede
255.255.255.0
Roteador
192.168.0.1
Renovar Concessão



Para deixar mais claro ainda, eu olhei nas configurações de rede do meu smartphone para descobrir qual era o IP dele: **192.168.0.20**. **Como meu celular está conectado na minha Wi-Fi, ele faz parte da minha rede doméstica, logo esse também possui um IP Privado ou Local.** Em outras palavras, eu possuo sete equipamentos na minha casa e cada um possui um endereço privado diferente. *Professor, eu ainda não entendi...*

Galera, a imagem ao lado representa a configuração básica da maioria das redes que temos em nossas casas. No caso, existem quatro dispositivos diferentes conectados a um equipamento que faz o papel de modem e/ou roteador e que se conecta à internet. Vejam se na casa de vocês não é exatamente dessa maneira...



Na minha casa é assim: dois computadores e um notebook estão conectados via cabo ao modem/roteador e os outros dispositivos também estão conectados a ele, porém via Wi-Fi. Note que eu disse que o endereço do meu computador era **192.168.0.17** e o endereço do meu smartphone era **192.168.0.20**. **Ambos esses endereços estão dentro da faixa de endereços privados, logo eles não existem na internet – existem apenas na rede interna.**

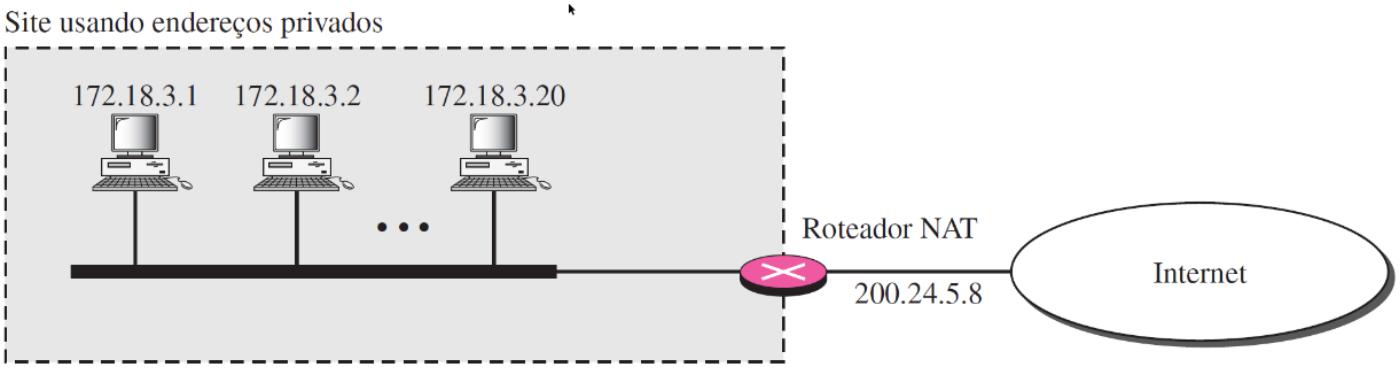
Vocês sabem que todo dispositivo em uma rede precisa ter um endereço IP. *Ora, o modem/roteador não é um dispositivo?* Sim, logo ele precisa ter um endereço IP! *Sabe qual é o endereço dele?* **189.6.109.248**. Esse endereço está contido em alguma das faixas de endereços

privados? Não, logo ele é um endereço público. Então, a minha rede tem nove equipamentos – cada um com seu endereço pertencente a faixa de endereços privados.

Já o meu roteador é o único dispositivo da minha rede local com um endereço pertencente a faixa de endereços públicos. *Legal, mas como eu faço para que meus equipamentos se comuniquem com a internet se o endereço deles é privado, portanto não existe na internet?* Agora vem à tona a criação genial dos engenheiros de redes: Network Address Translation (NAT). Trata-se de um recurso utilizado em roteadores e dispositivos de rede para traduzir endereços de uma rede para outra.

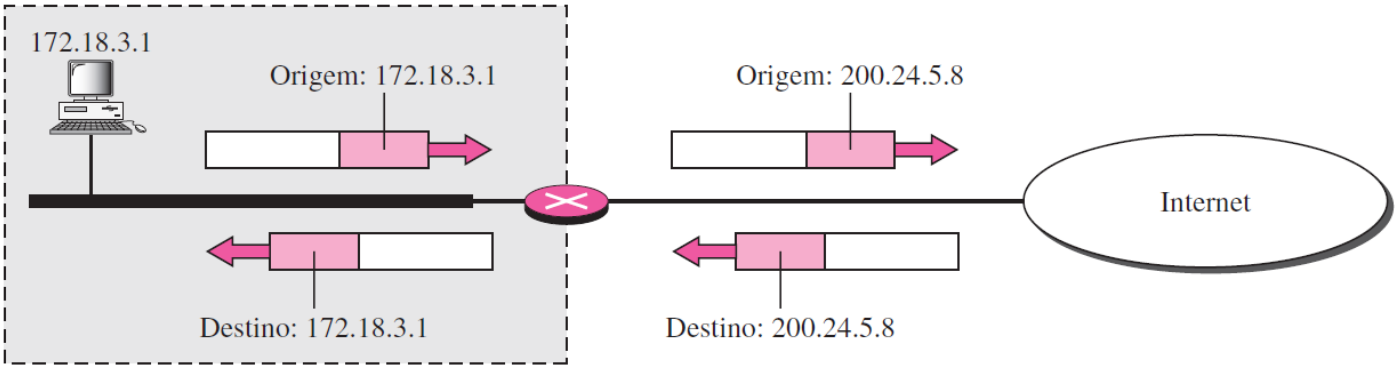
Essa tecnologia desempenha um papel crucial em permitir que dispositivos de uma rede privada se comuniquem com a internet. **Ela permite a um usuário ter internamente em sua rede doméstica uma grande quantidade de endereços privados e, externamente, possuir apenas um endereço público.** Dessa forma, qualquer rede doméstica pode utilizar um endereço da faixa de endereços privados sem a necessidade de pedir permissão para provedores de internet.

Eu disse para vocês diversas vezes que não podem existir equipamentos com o mesmo endereço IP em uma mesma rede. Ora, se meu computador é **192.168.0.17** na minha rede local e o seu também é **192.168.0.17** na sua rede local, não há nenhum problema porque estamos em redes diferentes. Logo, sempre que um pacote de dados sai da rede privada para a internet, ele tem seu endereço de origem substituído pelo endereço do roteador:

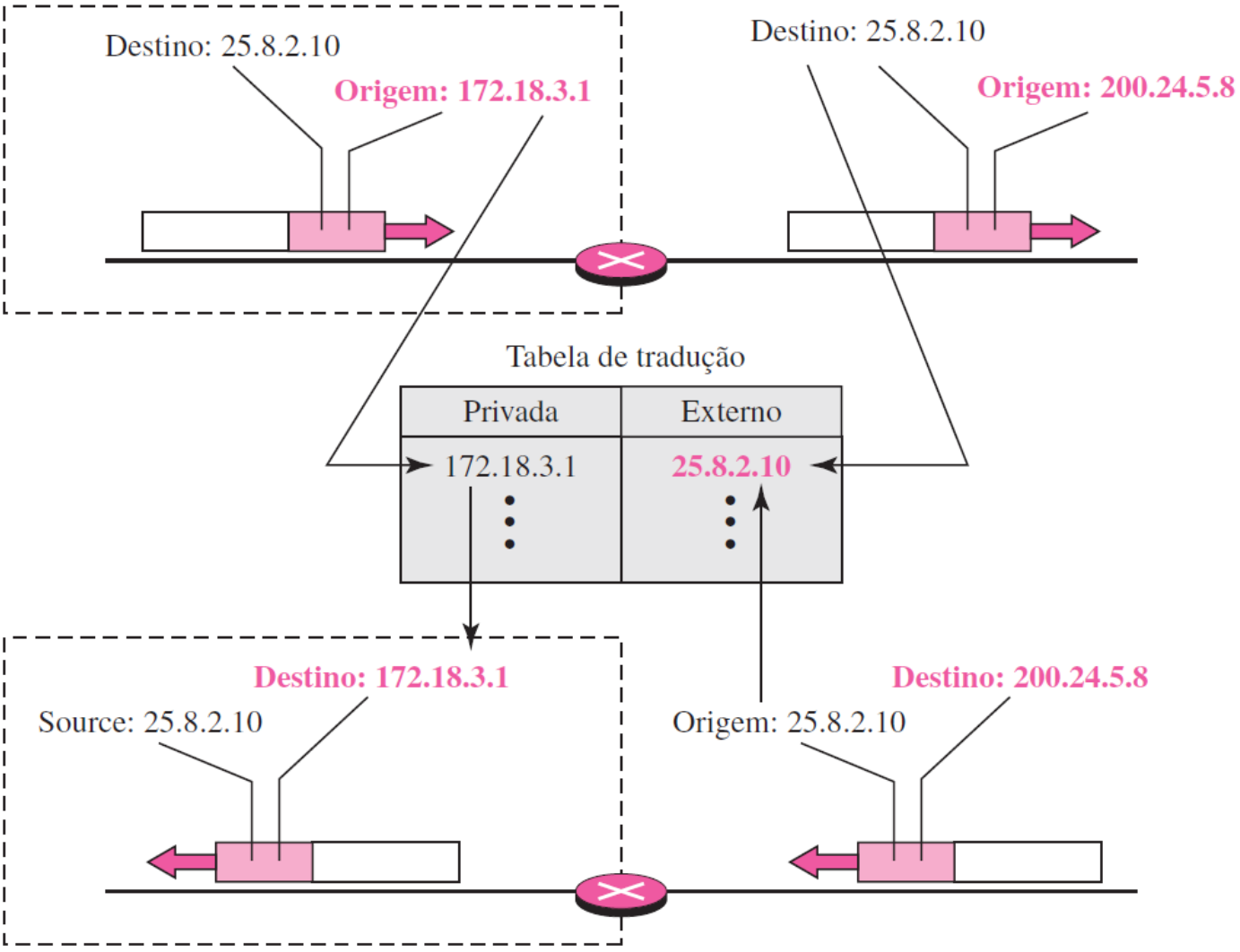


Na imagem acima, existem 20 equipamentos cujos endereços privados variam do **172.18.3.1** até **172.18.3.20**. No entanto, sempre que qualquer pacote sai dessa rede a partir de qualquer equipamento e acessa a internet, ele sai com um único endereço público: **200.24.5.8**. **Dados provenientes da internet para os equipamentos da rede interna sofrem o processo inverso – o endereço público é substituído pelo endereço privado específico da máquina destinatária.**

Professor, como ele sabe para qual máquina os dados devem ser enviados? Para tal, o NAT armazena uma tabela de tradução:



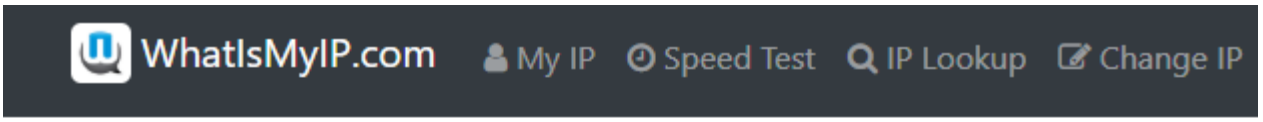
A tabela de tradução apresenta apenas duas colunas: o endereço privado e o endereço público. Quando um pacote de dados sai da rede interna para a rede pública (internet), o roteador armazena na tabela tanto o endereço de origem (privado) quanto o endereço de destino (público). **Quando a máquina de destino envia uma resposta para a máquina da rede interna, o roteador consulta a tabela e descobre o endereço privado que deve receber os dados.**



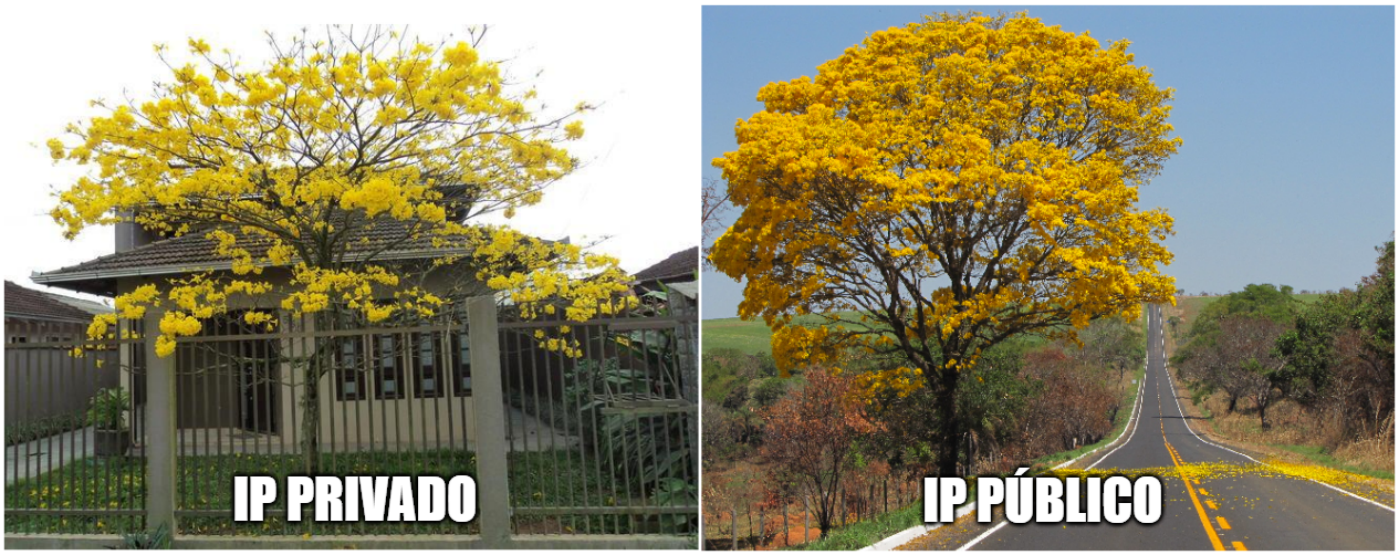
Na imagem acima, um pacote de dados sai da rede interna com endereço privado de origem 172.18.3.1 com destino a máquina da rede externa com endereço público de destino 25.8.2.10. Quando ele passa pelo roteador, o NAT armazena na tabela o endereço privado/interno e o endereço público/externo. Note também que ao passar pelo roteador, o endereço de origem muda de 172.18.3.1 para 200.24.5.8, porque esse é o endereço do roteador.

Na volta, um pacote de dados cujo endereço público de origem é 25.8.2.10 tem como endereço de destino 200.24.5.8. Quando esse pacote chega ao roteador, o NAT consulta quem havia enviado dados para o endereço 25.8.2.10 e descobre que havia sido a máquina da rede interna cujo endereço privado era 172.18.3.1, logo ele substitui o endereço do roteador 200.24.5.8 por 172.18.3.1. Com isso, nós aumentamos absurdamente a quantidade de equipamentos sem esgotar os endereços.

Professor, há uma maneira de descobrir meu IP público? Sim, basta acessar www.whatismyip.com [4]. Vejam que esse site informa que meu IP público é: **189.6.109.248**.



Em suma: o NAT é responsável por traduzir **endereços privados** (que existem apenas dentro de redes internas) para **endereços públicos** (que existem na internet).



#VamosPraticar#

(FUNDATEC / PROCERGS – 2023) O NAT (Network Address Translation) surgiu para resolver de forma rápida, não ideal e em curto prazo o problema de:

a) Baixo tráfego de dados na Internet.

b) Vulnerabilidade a novos vírus.

c) Esgotamento de endereços IP na Internet.

d) Padronização dos protocolos de camada física.

e) Acúmulo de dados na LAN.

Comentários: NAT foi uma solução implementada para lidar com o esgotamento de endereços IP na Internet. Com a expansão da Internet e a quantidade limitada de endereços IP disponíveis no IPv4, o NAT permite que múltiplos dispositivos em uma rede local compartilhem um único endereço IP público. Isso é feito traduzindo os endereços IP privados (usados internamente na rede) em um endereço IP público para comunicação externa (Letra C).

#VamosPraticar#

Para quem não entendeu como funciona esse recurso, vejamos uma analogia: imaginem um edifício de apartamentos onde cada apartamento representa um dispositivo em uma rede doméstica.

- **Endereços IP Privado (Número do Apartamento):** cada apartamento tem seu próprio número (Ex: Apartamento 503), representando um Endereço IP Privado (Interno) na rede privada. Quando os moradores se comunicam entre si, eles utilizam seus números de apartamento.

- **Endereços IP Público (Endereço do Edifício):** quando um morador precisa enviar uma carta para fora do edifício (acessar a internet), ele dá a carta ao porteiro (Roteador NAT). O porteiro usa o endereço do edifício (Endereço IP Público) para enviar a carta ao mundo exterior.

- **Tradução de Endereços:** o porteiro, ao receber as respostas do mundo exterior (dados advindos da internet), lê o número do apartamento (Endereço IP Interno) na carta e a entrega no apartamento do morador correto.

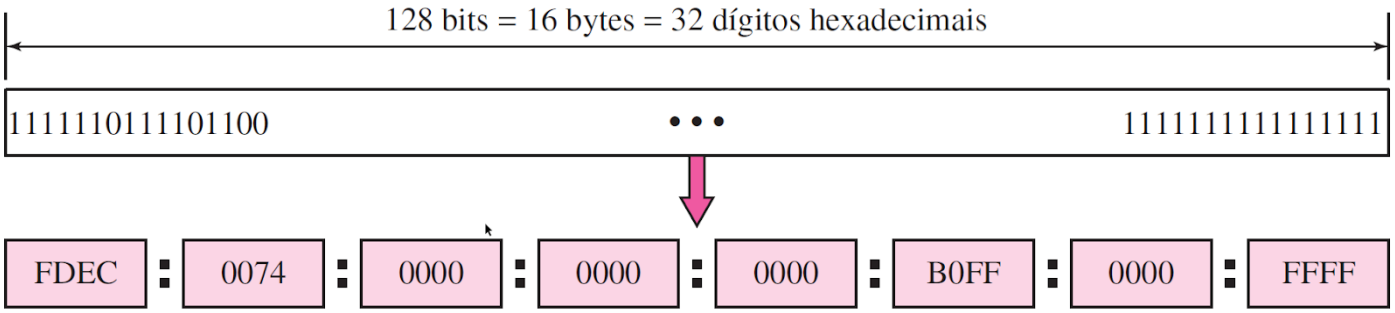
Essa pequena analogia demonstra como o NAT atua como um intermediário entre a rede interna (doméstica) e a rede externa (internet), permitindo que vários dispositivos em uma rede privada compartilhem um único Endereço IP (público) para se comunicar fora da rede. **Esse recurso, semelhante a um porteiro de um edifício de apartamentos, ajuda na eficiência e na segurança da comunicação.**

b) IPv6 (Versão 6):

O IPv4 foi implementado em 1983, quando a internet ainda estava engatinhando. Nenhum engenheiro de redes imaginou que teríamos em pouco tempo uma quantidade tão absurda de equipamentos no mundo acessando a internet. Nós estávamos avançando em máxima velocidade ao esgotamento total de endereços IP. **Era evidente: endereços não são infinitos – eles são recursos escassos como qualquer outro...**
Conforme acabamos de ver, surgiram soluções de curto prazo para ajudar a resolver o problema de esgotamento de endereços (Ex: NAT). No entanto, a escassez de endereços não era o único problema! Havia outros, tais como a falta de tratamento específico para transmissão de áudio/vídeo em tempo real e a criptografia/autenticação de dados para algumas aplicações. Tudo isso serviu de motivação para a criação de uma nova versão do Protocolo IP: **IPv6 (Versão 6)**.

A nova versão possui 128 Bits, logo temos até **2^{128}** possíveis endereços ou **340 undecilhões** de endereços ou 340.282.366.920.938.000.000.000.000.000. 000.000.000 de endereços!

No IPv4, decidiu-se utilizar uma representação decimal de 32 bits para facilitar a configuração! Ainda que fizéssemos isso com o IPv6, teríamos uma quantidade imensa de números. Dessa forma, **optou-se por utilizar uma representação com hexadecimal**, que necessita de todos os números e mais algumas letras: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F. Dividem-se 128 Bits em 8 grupos de 16 Bits (seção de 4 hexadecimais), separados por dois-pontos.



#VamosPraticar#

(FCC / AL-AP – 2020) Com o advento do IPv6, os Desenvolvedores de Sistemas terão que se acostumar com a nova representação dos endereços. Por exemplo, um endereço IPv6

a) apresenta a mesma representação do IPv4, porém com 16 grupos de 8 bits, em vez dos 4 grupos de 8 bits do IPv4.

b) possui oito grupos de 16 bits.

c) utiliza apenas caracteres minúsculos, não sendo aceitos os maiúsculos.

d) utiliza mais dígitos do que o IPv4, porém, ambas as representações separam os grupos de bits com um ponto (“.”).

e) utiliza o sistema octal para representar os dígitos.

Comentários: (a) Errado. Enquanto o IPv4 utiliza 4 grupos de 8 bits (totalizando 32 bits) representados em decimais, o IPv6 utiliza 128 bits, divididos em 8 grupos de 16 bits, e é representado em hexadecimal, não em grupos de 8 bits; (b) Correto. O IPv6 é composto por 128 bits, divididos em 8 grupos de 16 bits cada. Cada grupo é representado por 4 dígitos hexadecimais; (c) Errado. Não há distinção entre maiúsculas e minúsculas na representação de endereços IPv6; (d) Errado. Os grupos em um endereço IPv6 são separados por dois-pontos (:) e não por pontos; (e) Errado. O IPv6 usa o sistema hexadecimal para representar os dígitos, não o sistema octal. Hexadecimal é uma base-16, que inclui os dígitos de 0 a 9 e as letras de A a F (Letra B).

#VamosPraticar#

O IPv6 não possui o conceito de classes e nem endereço de *broadcast*. Além disso, como o endereço ainda fica grande com o hexadecimal, há algumas formas de abreviar: zeros não significativos de uma seção (quatro dígitos entre dois-pontos) podem ser omitidos, sendo que

apenas os zeros não significativos podem ser omitidos e, não, os zeros significativos. Na tabela abaixo, temos um exemplo:

ENDEREÇO ORIGINAL
FDEC:0074:0000:0000:0000:B0FF:0000:FFF0
ENDEREÇO ABREVIADO
FDEC:74:0:0:0:B0FF:0:FFF0
ENDEREÇO MAIS ABREVIADO
FDEC:74::B0FF:0:FFF0

Usando-se essa forma de abreviação, 0074 pode ser escrito como 74, 000F como F e 0000 como 0. Observe que se tivéssemos o número **3210**, por exemplo, não poderia ser abreviado. Outras formas de abreviações são possíveis se existirem seções consecutivas formadas somente por zeros. **Podemos eliminar todos os zeros e substituí-los por um dois-pontos duplo**. Note que esse tipo de abreviação é permitido apenas uma vez por endereço (Ex: não pode 2001:C00**::**5400**::**9).

Se existirem duas ocorrências de seções de zeros, apenas uma delas pode ser abreviada. A reexpansão do endereço abreviado é muito simples: devemos alinhar as partes não abreviadas e inserir zeros para obter o endereço original expandido. É interessante notar também que o IPv6 permite também o endereçamento local, isto é, endereços usados em redes privadas. Por fim, o IPv6 não pode se comunicar diretamente com o IPv4, mas existem diversas estratégias indiretas.

ENDEREÇO ORIGINAL
2001:0C00:0000:0000:5400:0000:0000:0009
ENDEREÇO ABREVIADO
2001:C00:0:0:5400:0:0:9
ENDEREÇO MAIS ABREVIADO
2001:C00::5400:0:0:9 ou 2001:C00:0:0:5400::9

NÃO PODE SER ABREVIADO
2001:C00::5400::9

ICMP (INTERNET CONTROL MESSAGE PROTOCOL)

INCIDÊNCIA EM PROVA: BAIXÍSSIMA

Internet control message protocol (icmp)
Protocolo da camada de rede responsável por enviar mensagens de erro e mensagens operacionais indicando, por exemplo, que um serviço não está disponível ou que um roteador ou host não pode ser alcançado. Ele Inclui tipos de mensagens como “destino inalcançável”, ”redirecionamento”, ”tempo excedido”, entre outros. Esse protocolo é amplamente utilizado para diagnóstico de rede e geração de erros, funcionando intimamente com o protocolo IP, para relatar erros e outras informações relevantes.

Nós já sabemos que o protocolo IP fornece serviços não confiáveis de entrega de pacotes. Ele foi projetado dessa forma para utilizar os recursos da rede de forma mais eficiente, oferecendo serviços de entrega de melhor esforço que possibilitam encaminhar um pacote desde sua origem até seu destino final. No entanto, ele apresenta duas deficiências: **falta de controle de erros e falta de mecanismos de notificação de erros.**

Agora o que acontece quando algo dá errado na entrega de um pacote ao destinatário? E se um roteador não conseguir encontrar um caminho até o destino final? O que acontece se houver um problema nos cabos de Internet? Estes são alguns exemplos de situações nas quais ocorreram erros! **O protocolo IP não apresenta mecanismos integrados para notificar erros ao remetente dos dados.** *E agora, o que fazer?*

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [versão 10.0.17763.914]
(c) 2018 Microsoft Corporation. Todos os direitos reservados.

C:\Users\Adm>ping www.estrategiaconcursos.com.br

Disparando www.estrategiaconcursos.com.br [2606:4700::6811:4343] com 32 bytes de dados:
Resposta de 2606:4700::6811:4343: tempo=140ms
Resposta de 2606:4700::6811:4343: tempo=225ms
Resposta de 2606:4700::6811:4343: tempo=142ms
Resposta de 2606:4700::6811:4343: tempo=177ms

Estatísticas do Ping para 2606:4700::6811:4343:
    Pacotes: Enviados = 4, Recebidos = 4, Perdidos = 0 (0% de
             perda),
Aproximar um número redondo de vezes em milissegundos:
    Mínimo = 140ms, Máximo = 225ms, Média = 171ms

C:\Users\Adm>
```

O **ICMP (Internet Control Message Protocol)** foi desenvolvido para suprir essas deficiências – **ele é um protocolo auxiliar do protocolo IP.** Trata-se de um protocolo da camada de Internet/Rede da Arquitetura TCP/IP, sendo utilizado para comunicar a ocorrência de situações anormais na transferência de um pacote, gerando relatórios de erros à fonte original e respondendo às consultas a respeito do estado das máquinas da rede e roteadores.

Na imagem acima, eu executo o comando ping. **Esse comando utiliza o protocolo ICMP para verificar a conexão com uma máquina qualquer.** Nesse caso, eu tentei acessar o servidor do Estratégia Concursos em *www.estrategiaconcursos.com.br* [5]. Notem que ele informa que foram enviados 4 pacotes para o servidor e 4 foram recebidos, logo não houve perda. Ocorreu tudo muito rápido (média de 171 milissegundos) e foi um sucesso.

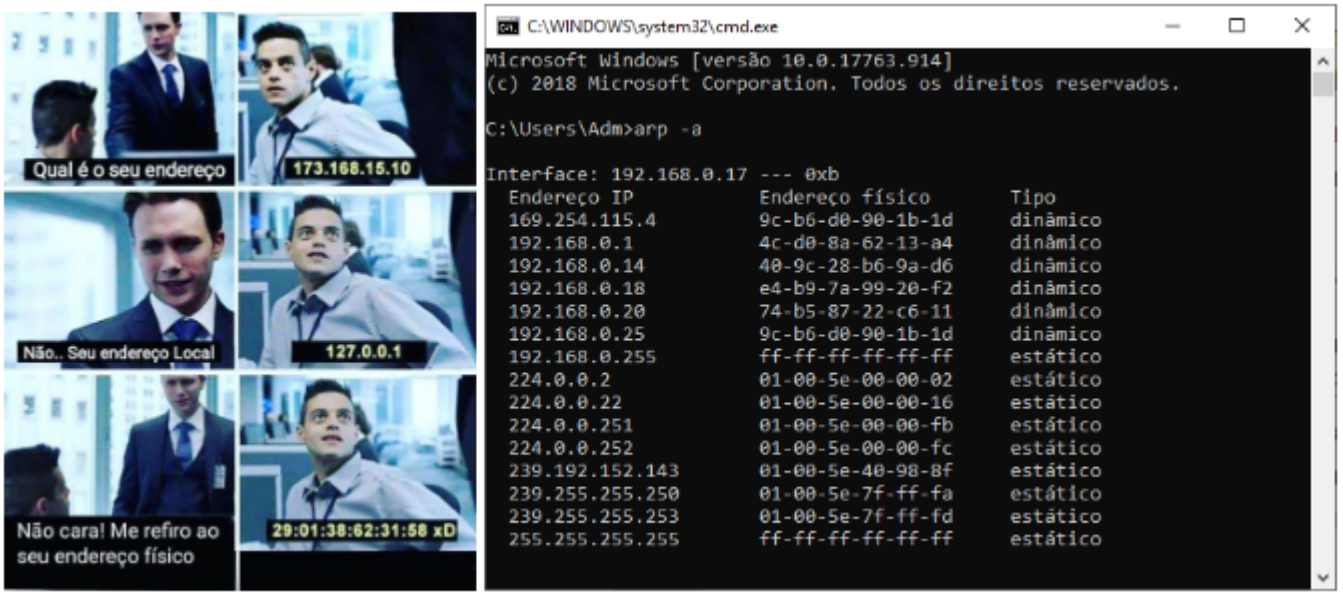
ARP (ADDRESS RESOLUTION PROTOCOL)

INCIDÊNCIA EM PROVA: BAIXÍSSIMA
Address resolution protocol (ARP)
Protocolo da camada de rede utilizado para mapear Endereços IP para Endereços MAC em redes locais, sendo fundamental para o funcionamento de redes IPv4. Ele é responsável por enviar uma requisição na rede local para descobrir o Endereço MAC correspondente a um Endereço IP específico. Os dispositivos na rede respondem com seus endereços MAC se o endereço IP solicitado corresponder ao seu.

Protocolo da Camada de Rede/Internet, ele é responsável por manter uma tabela de conversão de endereços lógicos em endereços físicos. Vocês devem se lembrar que endereço lógico é o endereço IP e endereço físico é o endereço MAC. **Esse protocolo mantém uma tabela de**

mapeamento entre endereços IP (Camada de Rede) e endereços MAC (Camada de Enlace). *Onde eu encontro essa tabela, professor?*

No *prompt* de comando do sistema operacional, se você digitar **arp -a**, você verá a tabela e todas as suas entradas, conforme imagem a seguir. Note que temos uma coluna com Endereço IP e outra com Endereço Físico. **Existe também o Reverse ARP (RARP), que é responsável por fazer o sentido contrário, isto é, ele mapeia endereços MAC (Camada de Enlace) para endereços IP (Camada de Rede). Notem que o Endereço MAC tem formato XX-XX-XX-XX-XX-XX.**



#Vamospraticar#

(FEPESE / Prefeitura de Balneário Camboriú-SC – 2023) Qual a função do protocolo de rede ARP?

a) A resolução de endereços IP em endereços MAC.

b) A resolução de endereços MAC em endereços físicos de placas de rede.

c) A resolução de endereços FQDN em endereços IP.

d) Estabelecer conexões seguras de ponta a ponta, independente da quantidade de nós na rede.

e) Estabelecer rotas automáticas IP com base em regras de menor custo/quantidade de nós na rede.

Comentários: o ARP é um protocolo que faz a resolução de Endereços IP em Endereços MAC (Letra A).

#VamosPraticar#

Protocolos da Camada de Transporte

TCP (TRANSMISSION CONTROL PROTOCOL)

INCIDÊNCIA EM PROVA: ALTA
TRANSMISSION CONTROL PROTOCOL (TCP)
Protocolo da camada de transporte, considerado confiável e orientado à conexão. Ele utiliza portas para estabelecer conexões, utiliza controle de fluxo para evitar congestionamento na rede, permite a transferência de dados bidirecional e confirma o recebimento de pacotes, retransmitindo os que não são confirmados. Além disso, ele garante que os pacotes cheguem na ordem correta e utiliza a soma de verificação para detectar erros nos dados recebidos. O TCP é amplamente utilizado em aplicações que requerem entrega garantida de dados, como navegadores web e e-mail.

Nós já sabemos que o Protocolo IP é classificado como não-confiável porque não oferece garantias de entrega de pacotes, sequenciamento de pacotes ou proteção contra duplicatas. **Para resolver esse problema de confiabilidade, nós temos um outro protocolo na camada de transporte chamado TCP (*Transmission Control Protocol*).** Por meio dele, é possível superar as limitações do Protocolo IP e oferecer uma comunicação confiável.

TCP: Funcionamento

O Protocolo de Controle de Transmissão (TCP) é um protocolo confiável, pois garante que os dados serão entregues íntegros e em ordem. Logo, se eu quero garantir que meu pacote chegará ao seu destino final, eu devo usar tanto o IP (protocolo que vai levar o pacote por várias redes) quanto o TCP (que vai garantir a entrega do pacote). Para tal, encapsula-se o TCP dentro do pacote IP. *Como é, Diego?* Isso mesmo! O TCP vai dentro do IP controlando e monitorando tudo...

O IP não estabelece um contato com o destino antes de enviar os pacotes, não é capaz de garantir a entrega dos dados, não é capaz de predizer quão congestionada estará uma rede e não é capaz controlar o fluxo de pacotes enviados para o destinatário. **Já o TCP é um protocolo orientado à conexão e confiável que faz o controle de congestionamento/fluxo e ainda permite a comunicação fim-a-fim**. Vamos entender isso melhor...

TCP: Características

a) Orientado a Conexões

O TCP comunica o destinatário que enviará pacotes antes de enviá-los de fato! *Como assim, Diego?* Imaginem que eu moro em uma casa pequena e quero me desfazer de algumas coisas para sobrar mais espaço em casa. Para tal, eu tenho a ideia de armazenar tudo em pacotes e deixá-los na casa do meu pai – que é bem mais espaçosa. Antes de simplesmente enviar os pacotes para o meu pai, eu entro em contato:

- Oi, pai! Como você está?

- Tudo ótimo, filho! O que você manda?

- Eu queria te enviar 100 pacotes para armazenar na sua casa. Pode ser?

- Pode, sim! Sem problemas.

- Eu vou começar enviando dez pacotes agora. Ok?

- Ok! Estou pronto para receber os dez pacotes agora!

...

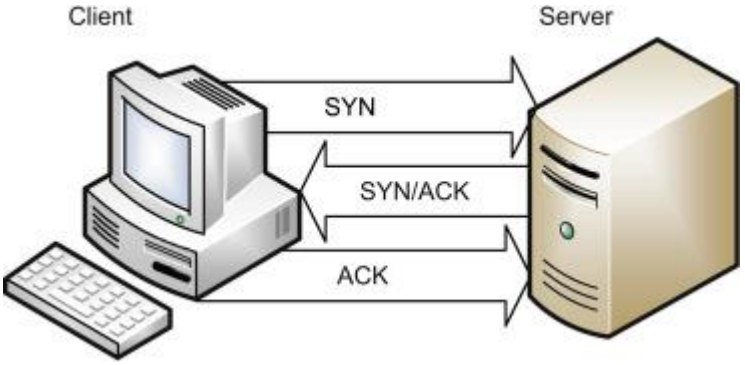
Vocês podem notar que, antes de enviar os pacotes, eu bati um papo com meu pai e expliquei a situação de forma que ele ficasse preparado. Se eu falasse que iria enviar naquele momento dez pacotes e meu pai não recebesse nada, ele me avisaria que não havia recebido e eu poderia verificar o que aconteceu no meio do caminho. **Por meio desse mecanismo, é possível garantir que – ao final da conexão – todos os pacotes tenham sido recebidos.**

De maneira mais técnica, pode-se afirmar que – quando um ponto A quer enviar e receber dados a um ponto B – os dois estabelecem uma conexão virtual entre eles, depois os dados são efetivamente trocados em ambos os sentidos e a conexão é encerrada. Utilizar uma única conexão virtual para uma mensagem inteira facilita o processo de confirmação de recebimento, bem como a retransmissão de segmentos perdidos ou corrompidos.

Você poderia se perguntar como o TCP (que usa os serviços do IP, que é um protocolo sem conexão) pode ser orientado a conexão. O ponto é que se trata de uma conexão virtual e, não, física – logo o TCP opera em um nível mais alto. Ele utiliza os serviços do IP para transmitir segmentos individuais ao receptor, porém é ele quem controla a conexão em si. **Se um segmento for perdido ou corrompido, ele será retransmitido.** *Professor, como efetivamente ocorre essa conexão?*

O TCP transmite dados no modo full-duplex, logo dois processos estão aptos a transmitir segmentos entre si de forma simultânea. Isso implica que cada parte deve inicializar a comunicação e obter a aprovação da outra parte antes que quaisquer dados possam ser transferidos. No TCP, uma transmissão orientada a conexão requer três fases: estabelecimento da conexão, transferência de dados e encerramento da conexão. **Esse processo é chamado de Three-Way Handshake.**

Para estabelecer a conexão entre uma máquina A e uma máquina B, a máquina A envia um segmento de controle chamado SYN (que é como se fosse um "Alô"); a máquina B envia de volta outro segmento de controle chamado SYN/ACK (que é como se fosse um "Alô" de resposta); então a máquina A envia outro segmento de controle chamado ACK. Pronto... conexão estabelecida!



Em seguida, segmentos de dados podem ser trocados! *Que segmentos, professor?* Lembrem-se que os dados da camada de aplicação são subdivididos em segmentos pela camada de transporte. Logo, segmentos de dados serão trocados, mas o TCP sempre fará a confirmação de entrega dos dados – isso o torna mais lento, porém mais confiável. **Já o UDP não estabelece conexão alguma!**Ele envia os dados: *chegou?* Ótimo; *Não chegou?* Paciência! Isso o torna mais rápido, porém menos confiável.

b) Conexão Fim-a-Fim

Imaginem que na rota entre duas grandes capitais brasileiras existam dezenas de cidades. Nós podemos dizer que entre esses dois pontos existem milhares de caminhos possíveis. O TCP é capaz de criar uma conexão entre dois processos em uma máquina – fim-a-fim – ignorando quaisquer nós intermediários que existam entre emissor e destinatário da informação e focando-se apenas nos processos finais. **O IP é um protocolo host-a-host, já o TCP é um protocolo fim-a-fim**.
Lembrando que um processo se refere a um programa ou aplicação em execução em um computador que usa a rede para se comunicar.A natureza fim-a-fim (também chamada de processo a processo) do TCP assegura uma comunicação confiável e ordenada diretamente entre processos específicos, independentemente das características físicas e das rotas da rede subjacente. *Entendido?*

#VamosPraticar#

(FUNCAB / SEMAD – 2013) Na arquitetura de protocolos da Internet, o protocolo que oferece um serviço fim a fim confiável e orientado à conexão é o:

a) IP

b) ICMP

c) TCP

d) UDP

Comentários: o protocolo que oferece um serviço fim a fim confiável e orientado à conexão é o TCP (Letra C).

#VamosPraticar#

c) Controle de Fluxo

Imaginem que após vários dias enviando pacotes para o meu pai, eu passo na frente da casa dele e vejo uma montanha pacotes fora de casa porque ele ainda não conseguiu abrir espaço para armazenar os pacotes. Eu posso reduzir meu fluxo e enviar apenas a quantidade que ele consegue absorver de forma que ele não fique sobrecarregado. **O controle de fluxo previne o receptor de ficar sobrecarregado por meio de um mecanismo chamado Janela Deslizante.**

d) Controle de Congestionamento

Toda vez que meu pai recebe meus pacotes, ele me avisa que os recebeu. Se eu percebo que ele está demorando demais para receber os pacotes que eu estou enviando, eu posso concluir – por exemplo – que o tráfego está intenso e que o caminhão de entrega está em um congestionamento. E, assim, posso reduzir a quantidade de pacotes enviados. **O controle de congestionamento previne que a rede fique sobrecarregada.**

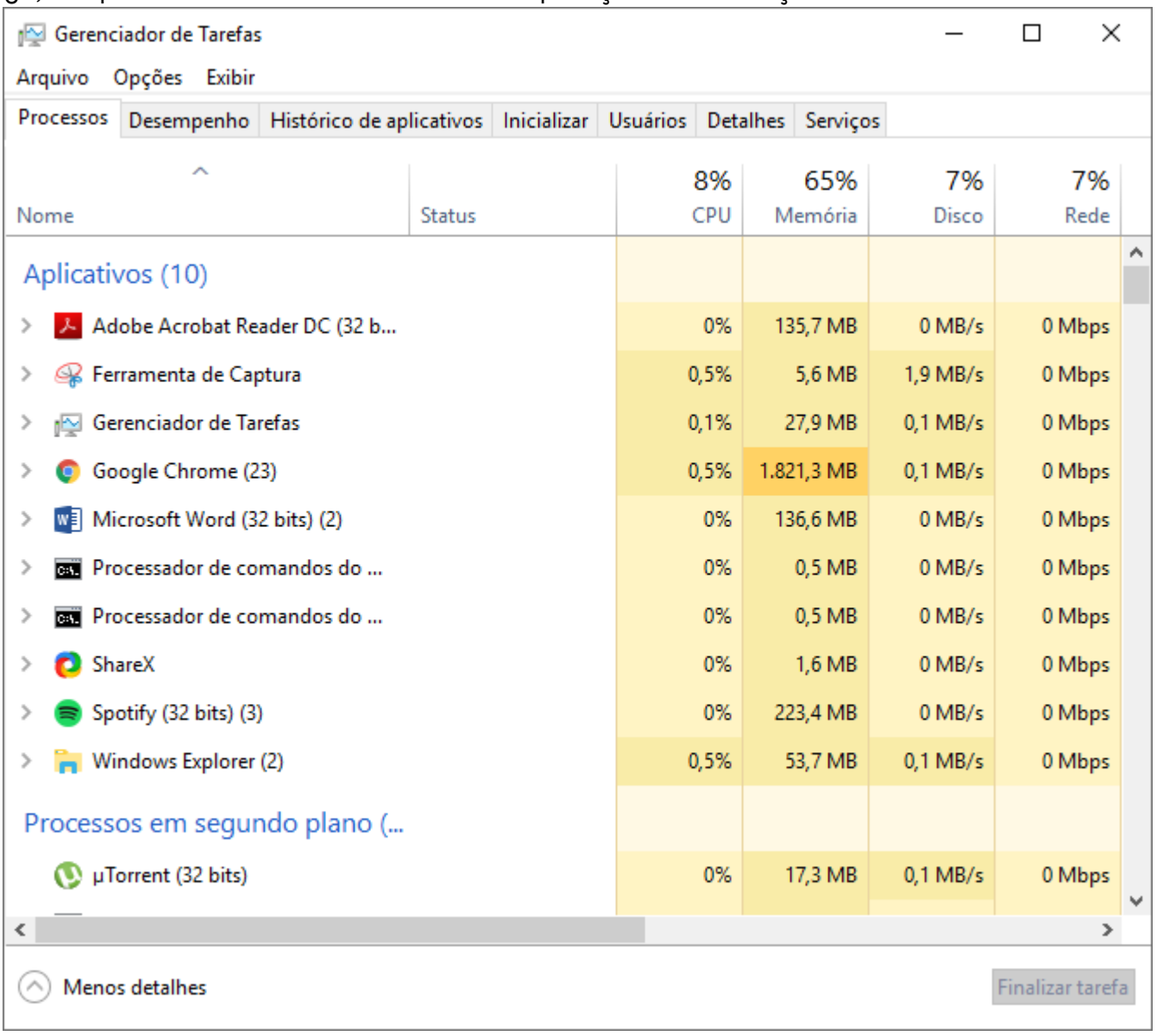
TCP: Portas

Para finalizar esse protocolo, vamos falar sobre portas. Para tal, vamos fazer uma analogia: imaginem que moram cinco pessoas na sua casa. Para que um carteiro lhe entregue um pacote, ele precisa do seu endereço. No entanto, esse endereço é compartilhado por toda a sua família. O carteiro não vai entrar na sua casa, procurar qual é o seu quarto, bater na sua porta e entregar um pacote diretamente para você.

Nesse sentido, podemos dizer que a sua casa possui um único endereço, mas ela possui diversos quartos, cada um com uma porta de modo que cada morador pode utilizar o serviço dos Correios. **Agora me acompanhem: imaginem que um pacote de dados viajou o planeta e, por meio do seu endereço IP, ele finalmente chegou ao seu computador**. Só que o seu

computador possui dezenas de processos diferentes em execução. *E aí, qual deles é o dono do pacote?*

Processos, professor? Sim, vamos fazer um teste! Pressionem de forma simultânea as teclas CTRL + SHIFT + ESC! Esse atalho abrirá o Gerenciador de Tarefas do Windows. **Observem que várias abas serão exibidas, sendo que a primeira delas é a aba de processos**. Nessa aba, estarão listados diversos processos que estão sendo executados atualmente em seu computador. No exemplo ao lado, no meu computador, há dez aplicativos abertos em primeiro plano no momento em que eu escrevo essa aula – cada um executando um ou mais processos. Logo, um processo é uma instância de uma aplicação em execução em determinado momento.



Quando nós falamos que a camada de transporte é fim-a-fim ou processo-a-processo, significa que ela pode garantir a entrega de segmentos entre processos rodando em máquinas diferentes – ignorando nós intermediários. Se chegam dados a uma máquina, ela não consegue saber quem é o remetente sem saber o número da porta. **Por meio do número da porta, ela consegue entregar os segmentos de dados diretamente ao destinatário correto.**

Na camada de enlace de dados, nós utilizamos o Endereço MAC; na camada de rede, nós utilizamos o Endereço IP; já na camada de transporte, nós utilizamos o Número da Porta para entregar dados para um entre vários processos que estejam em execução no destino.

Logo, o pacote percorreu o mundo inteiro em rotas terrestres e submarinas, chegou no meu computador e agora precisa saber qual processo deve recebê-lo. Para tal, ele precisa do número da porta!

Galera, o número da porta de destino é necessário para entrega e o número da porta de origem é necessário para resposta. *Professor, como são esses números?* Cara, são apenas números que variam entre zero e 65535. Cada uma pode ser usada por um programa ou serviço diferente, de forma que – em tese – poderíamos ter até 65536 serviços diferentes ativos simultaneamente em um mesmo servidor (tudo isso em um único Endereço IP).

Por exemplo: quando você está acessando uma página web por meio de um navegador, essa página web está armazenada em um servidor em algum lugar do mundo e o navegador está no seu computador. **O navegador é utilizado para acessar a web e o protocolo padrão da web é o HTTP!** Logo, para que o seu computador troque dados com o servidor que armazena a página do Estratégia Concursos, você precisará de uma porta. *Vocês se lembram do porquê?*

Porque um pacote encontrará o computador ou o servidor, mas não saberá qual processo é o dono do pacote. No caso do HTTP, a porta padrão é a 80! *Por que exatamente esse número?* Galera, tem uma organização chamada IANA (Internet Assigned Number Authority) responsável por definir e controlar algumas portas – ela definiu que a porta do HTTP é a 80! Logo, vamos fazer um último teste! Tentem acessar o endereço: ***http://www.estrategiaconcursos.com.br:80*** [6]
.

Notem que a página do Estratégia Concursos abrirá normalmente. Agora tentem com um número de porta diferente – por exemplo: ***http://www.estrategiaconcursos.com.br:21*** [7].

Não é possível acessar esse site

A página **http://www.estrategiaconcursos.com.br:21/** pode estar temporariamente indisponível ou pode ter sido movida permanentemente para um novo endereço da Web.

ERR_UNSAFE_PORT

Vejam que retornará um erro chamado **ERR_UNSAFE_PORT**. Esse erro é retornado quando você tenta acessar dados utilizando uma porta não recomendada pelo navegador. Em outras palavras, você está utilizando a porta errada! **Agora para fechar a nossa analogia: o endereço IP contém o endereço da sua casa, mas é a porta que determinará à qual quarto (processo) pertence o pacote**. *Bacana?* Então vamos ver uma listinha com as principais portas...

PROTOCOLO (CAMADA DE APLICAÇÃO)	PROTOCOLO (CAMADA DE TRANSPORTE)	NÚMERO DA PORTA
HTTP	TCP	80

HTTPS	TCP	443
POP3	TCP	110
SMTP	TCP	25/587
IMAP4	TCP	143
FTP	TCP	20/21
TELNET	TCP	23
SSH	TCP	22
DNS	TCP/UDP	53
DHCP	UDP	67/68
IRC	TCP	194

EM VERMELHO, OS PROTOCOLOS CUJO NÚMERO DE PORTA MAIS CAEM EM PROVA!

Galera, não precisa se desesperar para decorar todas essas portas! Eu coloquei em vermelho as principais, mas mesmo essas não caem com bastante frequência, logo analisem o custo-benefício de memorizar esse tipo de assunto. **Por fim, é importante falar sobre Data Protocol Unit (DPU) ou Unidade de Dados de Protocolos.** Cada camada possui um nome para sua unidade, um tipo de comunicação e um tipo de endereço (sendo *pacote* é um termo genérico para qualquer unidade):

CAMADas	Unidade de dados padrão	Tipo de comunicação	Tipo de endereço
FÍSICA	Bits	Ponto-a-Ponto	-
ENLACE	Quadros/Frames	Ponto-a-Ponto	Endereço Físico (MAC)
REDE	Datagramas	Host-a-Host	Endereço Lógico (IP)
TRANSPOrTE	Segmentos [8]	Fim-a-Fim	Endereço de Portas

SESSÃO	Mensagens	Fim-a-Fim	Endereços Específicos (URL)
APRESENTAÇÃO			
APLICAÇÃO			

#VamosPraticar#

(UFMT / UFMT – 2021) Um pacote da camada de transporte da pilha de protocolos é chamado de:

a) Quadros. b) Segmentos. c) Datagrama. d) Frames.

Comentários: (a) Errado. Esta terminologia é mais comum na camada de enlace, onde os dados são encapsulados em quadros; (b) Correto. Na camada de transporte, os pacotes são chamados de "segmentos". Essa camada divide os dados em segmentos para transmissão e adiciona informações de controle, como portas de origem e destino; (c) Errado. O termo "datagrama" geralmente é usado na camada de rede, onde os pacotes são referidos como datagramas; (d) Errado. Novamente, "frames" ou “quadros” é uma terminologia da camada de enlace, onde os dados são encapsulados em quadros (Letra B).

#VamosPraticar#

UDP (USER DATAGRAM PROTOCOL)

INCIDÊNCIA EM PROVA: BAIXÍSSIMA
User datagram protocol (udp)
Protocolo da camada de transporte, considerado sem conexão e utiliza portas para comunicação de forma similar ao TCP. Ele não possui controle de fluxo e permite a transferência de dados rápida, mas sem garantias de entrega, ordem ou integridade. Esse protocolo é considerado não confiável porque não é capaz de confirmar o recebimento de pacotes e não retransmite os pacotes perdidos. Ele também não reordena pacotes e realiza apenas verificações básicas de erros nos dados recebidos (mas não os corrige). Por fim, ele não requer estabelecimento de conexão antes da transferência de dados, sendo ideal para aplicações que requerem transmissão rápida, como streaming de vídeo e jogos online.

Protocolo da Camada de Transporte, ele fornece um serviço de entrega sem conexão e não-confiável (sem controle de fluxo e de congestionamento). Esse protocolo é praticamente o inverso do anterior – ele não adiciona nenhum controle adicional aos serviços de entrega do IP, exceto pelo fato de implementar a comunicação entre processos, em vez da comunicação entre hosts. Ele até realiza alguma verificação de erros de erros, mas de forma muito limitada.

Professor, se esse protocolo é tão simples assim, por que um processo iria querer usá-lo? Com as desvantagens vêm algumas vantagens! Por ser muito simples, ele tem um baixo overhead (tráfego adicional). **Se um processo quiser enviar uma pequena mensagem e não se preocupar muito com a confiabilidade, o UDP é uma boa escolha. Ele exige menor interação entre o emissor e o receptor do que quando utilizamos o TCP.**

Alguns contextos específicos não se preocupam se um pacote eventualmente for perdido, duplicado ou chegar fora de ordem. Se eu estou conversando com outra pessoa por áudio ou vídeo, perder um ou outro pacote de dados não causa problemas significativos – talvez eu perca uma palavra ou outra quando estou conversando por áudio com alguém; se eu estiver conversando por vídeo, pode ser que eu perca alguns quadros.

No entanto, não faz nenhum sentido tentar reenviar esses pacotes perdidos – como ocorre com o TCP. *Por que?* Porque nesses serviços *real-time* (tempo real), essas pequenas perdas são insignificantes. *Bacana?* **TCP e UDP possuem algumas vantagens e desvantagens em relação ao outro dependendo do contexto de utilização**. Para não ter mais confusão, vamos ver uma tabela comparativa entre TCP e UDP...

TCP	UDP
É comparativamente mais lento que o UDP	É comparativamente mais rápido que o TCP
Entregas confiáveis	Entregas não confiáveis (melhor esforço)
Orientado à conexão	Não orientado à conexão
Dados perdidos são retransmitidos	Dados perdidos não são retransmitidos.
Realiza controle de fluxo e congestionamento	Não realiza controle de fluxo e congestionamento
Tolera atrasos, mas não tolera perdas	Tolera perdas, mas não tolera atrasos
Envia dados em unicast	Envia dados em unicast, multicast ou broadcast
Oferece conexão ponto a ponto	Oferece conexão ponto a ponto ou ponto-multiponto

Bastante utilizada em e-mail, navegação, etc.	Bastante utilizada em VoIP, streaming, etc.

Apesar das diferenças, observem que todas são consequências da orientação à conexão. O TCP é orientado à conexão, logo suas entregas são confiáveis, visto que ele realiza controle de fluxo e congestionamento, além de retransmitir dados perdidos. **Para oferecer uma conexão confiável, ele somente consegue trabalhar com um remetente e um destinatário, logo oferece serviços ponto-a-ponto e unicast – apesar de permitir a transferência de dados full-duplex.**

Já o UDP não é orientado à conexão, logo suas entregas não são confiáveis – ele faz o máximo que pode, mas suas entregas não são garantidas. **Como ele não precisa de uma conexão confiável, ele pode trabalhar com serviços ponto-a-ponto ou ponto-multiponto, além de trabalhar em unicast, multicast e broadcast – e também em full-duplex. Logo, ele pode transferir dados de um remetente para um, alguns ou todos os destinatários.** Vejam uma famosa piada sobre UDP:

- Você quer ouvir uma piada sobre o TCP?

- Sim, eu quero ouvir uma piada sobre o TCP.

- Você está pronto para ouvir uma piada sobre o TCP?

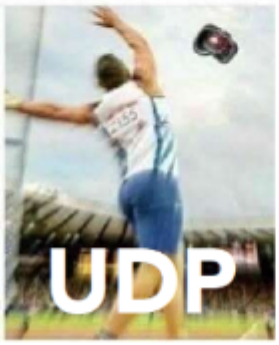
- Sim, estou pronto para ouvir uma piada sobre o TCP.

- Aqui está uma piada sobre o TCP.

- Você recebeu a piada sobre o TCP?

- Sim, eu recebi a piada sobre o TCP.

- Excelente. Você recebeu a piada sobre o TCP. Tchau!



Sinto dizer, mas se você estiver entendendo esses memes, você está em processo inicial de transformação em nerd; se estiver rindo desses memes, então você já está em estado avançado...

Protocolos da Camada de Aplicação

Protocolos de E-Mail

INCIDÊNCIA EM PROVA: ALTA

Correio Eletrônico (E-Mail) é uma forma de comunicação digital que permite aos usuários enviar e receber mensagens através de redes eletrônicas. O serviço de correio eletrônico é baseado em uma arquitetura cliente/servidor, isto é, uma arquitetura composta de máquinas responsáveis por oferecer serviços (por essa razão, é chamada de servidor) e de máquinas responsáveis por consumir serviços (por essa razão, é chamada de cliente).

No decorrer desse tema, vamos ver diversos termos que vocês estão acostumados, mas que podem gerar dúvidas. Dessa forma, vamos parar um pouquinho para detalhá-los:

Cliente de e-mail	Trata-se de uma **aplicação instalada em uma máquina local** que permite enviar/receber e-mails (Ex: Mozilla Thunderbird, Microsoft Outlook, etc);
Servidor de e-mail	Trata-se de uma **máquina especializada** que recebe e-mails de um cliente de e-mail ou de um webmail, e os envia para o servidor de e-mail de destino;

Provedor de e-mail	Trata-se de uma **empresa ou serviço** que hospeda e disponibiliza serviços de e-mail para outras empresas ou usuários finais (Ex: Gmail, Outlook, Yahoo, Uol, etc);
webmail	Trata-se de uma **aplicação hospedada em um servidor remoto** que permite enviar/receber e-mails (Ex: Outlook.com [9], Gmail.com [10], Yahoo.com [11], Uol.com [12], etc).

Os principais protocolos de correio eletrônico são: SMTP, POP e IMAP. Vamos vê-los resumidamente na tabela a seguir e depois entraremos nos detalhes de cada um:

PROTOCOLOS DE E-MAIL	DESCRIÇÃO
SMTP	Protocolo utilizado basicamente para enviar e-mails. Ele transfere mensagens de e-mail de um cliente para um servidor ou entre servidores. Funciona bem para a entrega de mensagens, mas não para recuperá-las.
POP	Protocolo projetado para recuperar e-mails de um servidor. Quando você o utiliza, os e-mails são baixados para o seu dispositivo e geralmente são excluídos do servidor. Isso é útil para acessar e-mails offline, mas pode ser limitante se você usar vários dispositivos, pois as mensagens estão disponíveis apenas no dispositivo onde foram baixadas inicialmente.
IMAP	Também usado para recuperar e-mails de um servidor, mas – diferentemente do anterior – ele mantém as mensagens no servidor. Isso permite que você acesse seus e-mails de vários dispositivos, mantendo tudo sincronizado. As mudanças feitas em um dispositivo (como ler ou excluir uma mensagem) são refletidas em todos os outros dispositivos.

SMTP	POP3	IMAP
ENVIAr	**Receber e COPIAr**	**Receber e ACESSAr**

#VamosPraticar#

(FAT / CEETEPS – 2023) Protocolos são regras definidas e precisas de uso da internet. Dessa forma, representam o conjunto de regras de como as coisas devem acontecer quando estamos navegando, recebendo ou enviando e-mail. São exemplos de protocolos:

I. Protocolo HTML, responsável pela navegação da internet.

II. Protocolos POP3 e IMAP, responsáveis pela recepção dos e-mails.

III. Protocolo SMTP, responsável pelo envio de e-mails.

É correto afirmar que:

a) as afirmativas I, II e III estão corretas.

b) somente a afirmativa I está correta.

c) somente a afirmativa II está correta.

d) somente a afirmativa III está correta.

e) somente as afirmativas II e III estão corretas.

Comentários: (I) Errado. HTML (Hypertext Markup Language) não é um protocolo, mas sim uma linguagem de marcação usada para criar e estruturar páginas na web. O protocolo responsável pela navegação na internet é o HTTP (Hypertext Transfer Protocol); (II) Correto. POP3 (Post Office Protocol version 3) e IMAP (Internet Message Access Protocol) são protocolos usados para receber e-mails de um servidor de e-mail; (III) Correto. SMTP (Simple Mail Transfer Protocol) é o protocolo padrão usado para enviar e-mails de um cliente para um servidor de e-mail e entre servidores de e-mail (Letra E).

#VamosPraticar#

E-Mail: SMTP

Simple mail transfer protocol (SMTP)
Protocolo da camada de aplicação responsável pelo envio de e-mails de um cliente para um servidor ou entre servidores de e-mail. Ele é bastante utilizado por clientes de e-mail e servidores de e-mail para a transmissão de mensagens de correio eletrônico, funcionando por meio de uma arquitetura cliente/servidor. Além disso, é interoperável com outros protocolos de e-mail (Ex: POP3 e IMAP) para uma funcionalidade de e-mail completa.

O SMTP é um protocolo da camada de aplicação utilizado para enviar mensagens de e-mail de um cliente de e-mail para um servidor de e-mail e entre servidores de e-mail em

uma rede de computadores. Quando um usuário envia um e-mail, o SMTP cuida de encaminhar essa mensagem do servidor de e-mail do remetente para o servidor de e-mail do destinatário. O SMTP é eficaz para enviar mensagens, mas não para recuperá-las ou armazená-las.

S	M	T	P
S	M	T	P

Ele também é utilizado para a comunicação entre servidores de e-mail, permitindo que eles passem e-mails de um para o outro até que a mensagem alcance o servidor de e-mail do destinatário final (veremos esse caso específico mais à frente). **O SMTP – em seu uso moderno – inclui mecanismos de autenticação para aumentar a segurança, ajudando a prevenir o abuso do sistema de e-mail, como o envio de spam.** Vejamos alguns cenários de utilização:

a) Cenário 1: troca de e-mails em um mesmo provedor

Vamos supor que Diego deseja enviar um e-mail para Renato e ambos possuem uma conta no mesmo provedor de e-mail, logo utilizarão o mesmo servidor de e-mail. Considere que o e-mail de Diego é *diego@gmail.com* [13] e o e-mail de Renato é *renato@gmail.com* [14]. **Notem que o domínio é o mesmo (gmail.com [15]), logo se trata do mesmo provedor de e-mail, portanto ambos acessam o mesmo servidor de e-mail.**

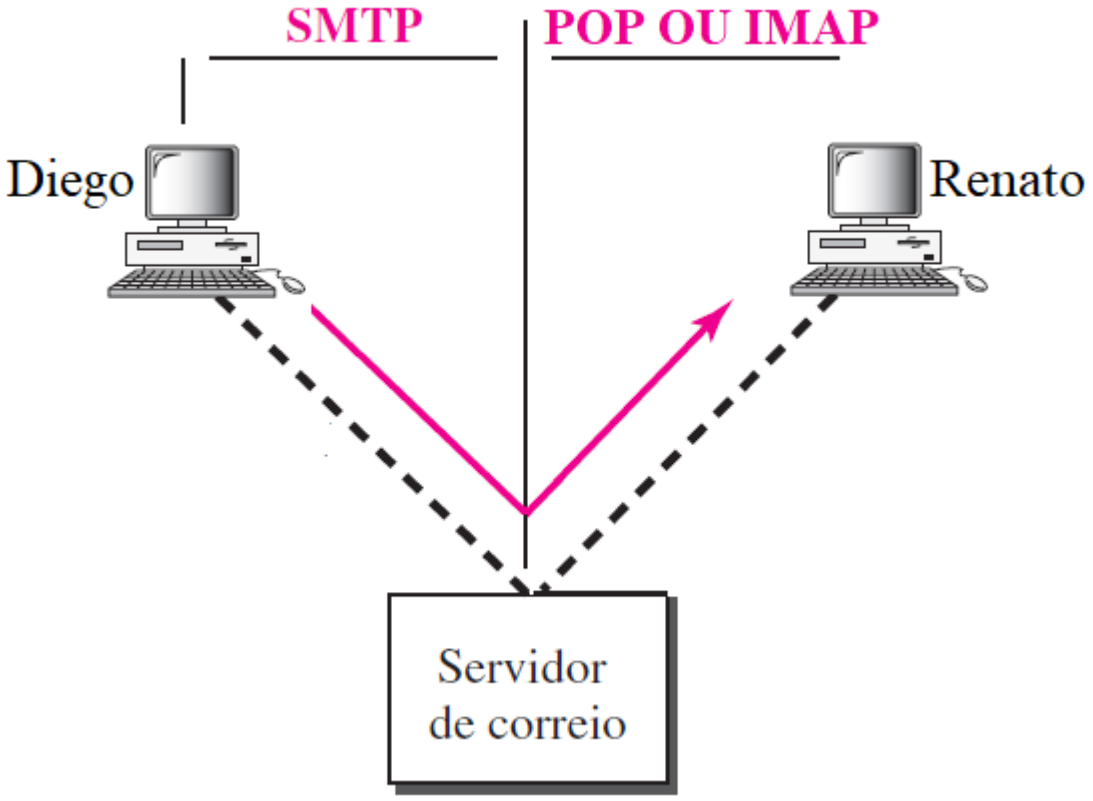
Quando Diego quiser enviar um e-mail para Renato, a mensagem não será encaminhada diretamente de um para o outro. *Por que?* Porque o serviço de correio eletrônico é baseado em um modelo cliente/servidor, logo o remetente e o destinatário não se comunicam de forma direta. Dessa forma, a mensagem de Diego deve passar pelo servidor de e-mail antes de chegar a Renato. *E o que o servidor faz?* Ele armazena a mensagem! *Aonde ele armazena?***Na caixa postal de Renato!**

Vamos fazer uma analogia: suponha que você trabalha viajando o país e não possui um endereço físico. Ainda assim, você pode precisar receber correspondências ou encomendas eventualmente. *E agora, o que fazer?* Você pode ir aos Correios e contratar um serviço de Caixa Postal. *O que é isso?* É um recipiente para receber correspondências e encomendas de maneiras prática, sem precisar ter um endereço fixo ou alguém em casa para recebê-los. No contexto de e-mails, a caixa postal tem o mesmo sentido.

A caixa postal de e-mail funciona exatamente assim: o servidor de e-mail armazenará a mensagem enviada por Diego na caixa postal de Renato. *Professor, quando o Renato vai ler o e-mail enviado?* Isso é irrelevante porque o serviço de e-mail é assíncrono, isto é, a comunicação não exige uma sincronia para ocorrer – ela pode ocorrer de maneira simplesmente dessincronizada. *Ainda não entendi muito bem, professor...*

Galera, um exemplo de serviço síncrono é um chat ou um telefonema: quando um fala, o outro deve estar disponível no mesmo momento para que possa responder à mensagem; caso contrário, a conversa não fluirá. Você não vai ligar para alguém, falar "alô" para ela responder só daqui duas horas! Um serviço assíncrono permite que o destinatário leia e responda quando bem entender (como nós fazemos com mensagem e áudio no Whatsapp). Então, vamos resumir...

Diego compõe uma mensagem no Gmail e a envia para Renato. O SMTP é utilizado para enviar esta mensagem do cliente de e-mail de Diego para o servidor de e-mail do Gmail. Uma vez que o servidor do Gmail recebe a mensagem, ele identifica que o destinatário, Renato, também está no Gmail. O servidor então processa a mensagem internamente, sem a necessidade de enviar a mensagem para outro servidor. A mensagem é colocada na caixa postal de Renato no Gmail, que pode acessá-la posteriormente.

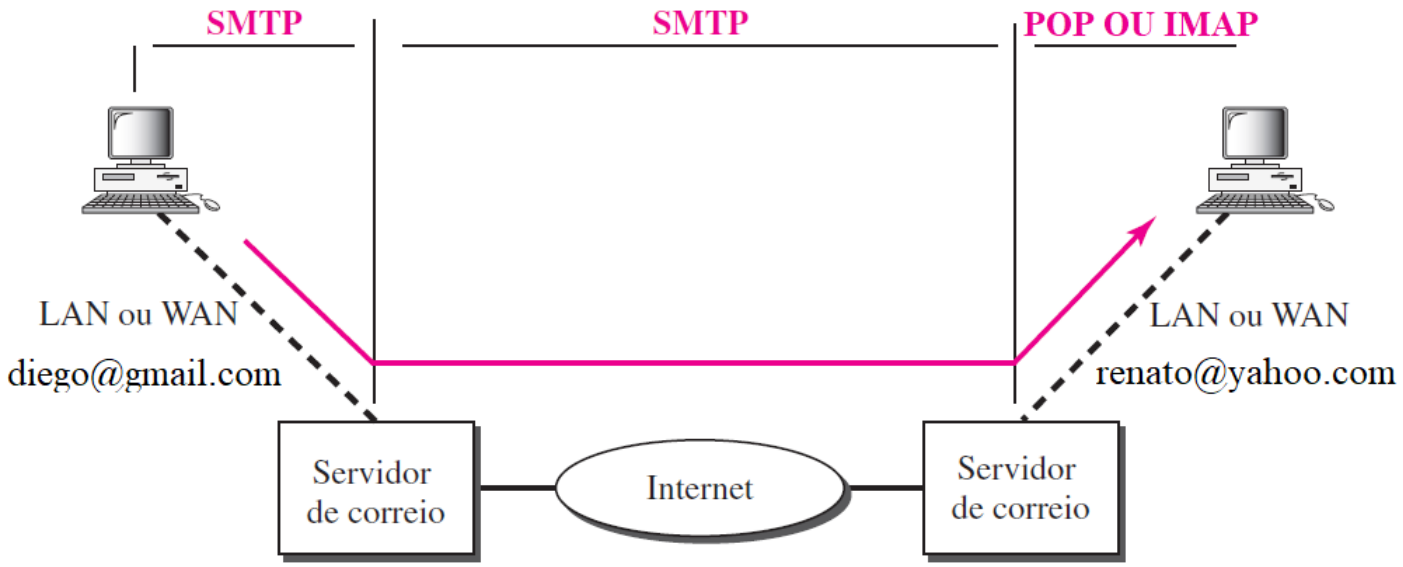


b) Cenário 2: troca de e-mails em provedores diferentes

Suponha agora que o e-mail de Diego é *diego@gmail.com* [16] e o e-mail de Renato é *renato@yahoo.com* [17]. Nesse caso, temos domínios diferentes, logo teremos provedores (e servidores) diferentes entre os usuários. Quando Diego enviar uma mensagem para Renato, a mensagem sai do seu programa cliente de e-mail e chega até o servidor de correio de origem (também chamado de servidor de saída).

O servidor de correio de origem analisa apenas o segmento que se encontra após o símbolo de @ para identificar o endereço de domínio de destino (renato@**yahoo.com** [18]). O servidor de saída – ainda por meio do SMTP – envia a mensagem para o servidor de correio de destino (também chamado de servidor de entrada). O servidor de correio de destino identifica a informação existente antes do símbolo @ (**renato**@yahoo.com [19]) e deposita a mensagem em sua respectiva caixa postal.

Quando Renato quiser, ele utiliza seu programa cliente de e-mail ou webmail para – por meio do POP3 ou IMAP – recuperar a mensagem e/ou armazená-la na máquina local. Vamos resumir...



Diego escreve e envia um e-mail para Renato por meio do Gmail. O SMTP transfere a mensagem para o servidor de e-mail do Gmail. Esse servidor também utiliza o SMTP para enviar a mensagem para o servidor de e-mail do Yahoo, que é o provedor de Renato. Este processo pode envolver a mensagem passando por vários servidores e redes de computadores na internet. Uma vez que o servidor do Yahoo receba a mensagem, ele a processa e entrega na caixa de Renato no Yahoo.

#VamosPraticar#

(OBJETIVA / Prefeitura de Canoas-RS – 2023) O serviço de correio eletrônico, ou Electronic Mail (E-Mail), é um dos serviços mais antigos e utilizados atualmente na rede. Para o envio de mensagens entre os servidores, o protocolo utilizado é o:

a) Simple Mail Transfer Protocol (SMTP).

b) Transmission Control Protocol (TCP).

c) Hypertext Transfer Protocol (HTTP).

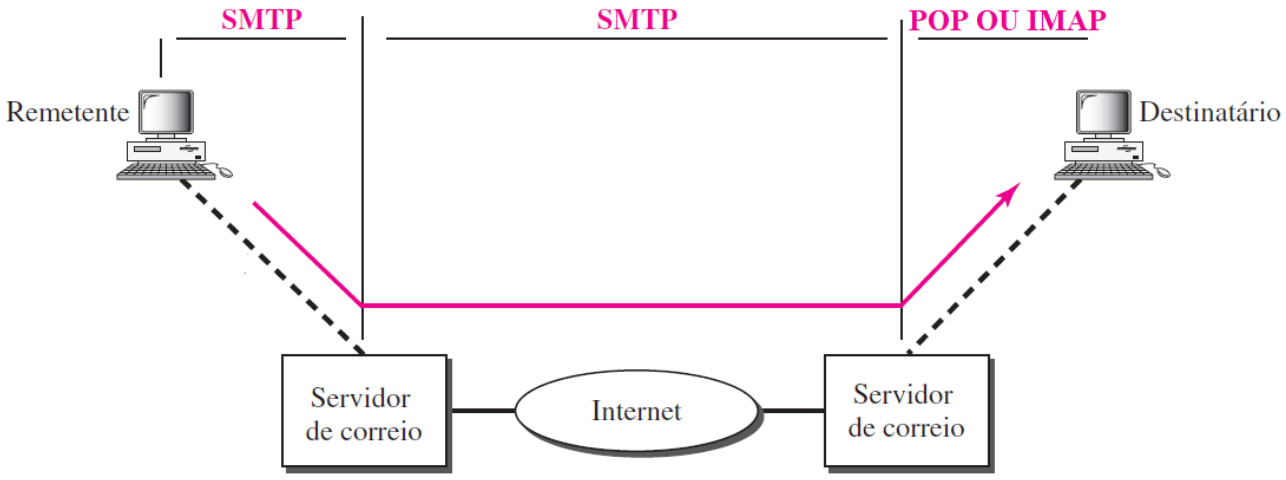
d) Hypertext Transfer Protocol Secure (HTTPS).

e) File Transfer Protocol (FTP).

Comentários: o protocolo utilizado para envio de mensagens entre servidores de e-mail é o SMTP (Letra A).

#VamosPraticar#

Vocês se lembram que eu falei que o SMTP também é utilizado para comunicação entre servidores? Bem, isso caiu apenas uma vez em prova, mas foi uma polêmica imensa! Nós já vimos exaustivamente que o SMTP é o principal protocolo de transferência de correio eletrônico através da rede. *Eu menti?* Não! **No entanto, ele também pode ser utilizado para receber e-mail em uma única situação**. Para entender melhor, vamos analisar a imagem seguinte:



Percebam que o remetente utiliza o protocolo SMTP para enviar uma mensagem de correio eletrônico. **No entanto, notem que na comunicação entre o servidor de correio eletrônico do remetente e do destinatário também é utilizado o SMTP**. Logo, nesse caso específico de comunicação entre servidores, ele é utilizado tanto para envio quanto para recebimento de correio eletrônico. Não é o padrão, é apenas nesse caso! *Bacana?*

E-Mail: POP

Post office protocol (pop)

Protocolo da camada de aplicação responsável por recuperar e-mails de um servidor de e-mail. Em regra, ele baixa os e-mails do servidor para o cliente local e os deleta do servidor, mas há outros modos de funcionamento. O POP3 suporta criptografia via SSL/TLS e autenticação através de usuário/senha, além de permitir a leitura de e-mails offline e controle limitado sobre as mensagens no servidor. Por outro lado, ele não sincroniza o estado da mensagem entre múltiplos dispositivos (lido/não lido, marcado/não marcado). Ele é menos flexível que IMAP, sendo ideal para usuários que acessam e-mail de um único dispositivo.

O POP3 é um protocolo da camada de aplicação criado como uma forma simplificada para fazer o download de mensagens da caixa postal de um servidor de correio eletrônico para a máquina do usuário. Por meio desse protocolo, Renato poderá acessar a caixa postal no servidor de correio remoto e baixar seus e-mails para a sua máquina local. Galera, o POP já foi mais popular (piada infame), mas é bem menos utilizado hoje em dia. *Por que, professor?*

Antigamente, o espaço de armazenamento dos servidores de correio eletrônico era bastante pequeno. Hoje em dia, qualquer provedor oferece uma conta gratuita com 15Gb de espaço de armazenamento. Há muito tempo, nem se você pagasse, você teria tanto espaço assim disponível. Era comum, inclusive, que os usuários tivessem que acessar seus e-mails todos os dias para evitar que a caixa de e-mails ficasse lotada e futuros e-mails não fossem recebidos.

O POP era extremamente útil porque ele permitia apagar a mensagem do servidor de correio eletrônico após a leitura pelo destinatário e armazená-la em sua máquina local. Dessa forma, o espaço de armazenamento era liberado para a chegada de novos e-mails no servidor. Na verdade, esse é o modo padrão de funcionamento desse protocolo, mas possui duas maneiras distintas de trabalhar com correio eletrônico.

No modo Delete/Download, ele remove as mensagens da caixa postal após a realização do download para a máquina local. Esse modo tem como vantagens poder organizar as mensagens recebidas e abrir espaço no servidor para o recebimento de novas mensagens. No entanto, o gerenciamento de e-mails se tornava complexo se o usuário utilizasse mais de um computador – além do risco de sua máquina ser infectada por um malware ou simplesmente ser furtada.

No modo Keep/Notification, ele permanece realizando o download dos e-mails para a máquina local, porém ele não os remove da caixa postal. Esse modo tem como vantagens manter um gerenciamento centralizado dos e-mails e não correr o risco de perda de dados porque os e-mails eram mantidos no servidor. No entanto, o armazenamento de e-mails poderia ultrapassar o espaço de armazenamento, resultando em um descarte de novos e-mails recebidos.

O POP3 era indicado para as pessoas não possuíam acesso fácil à Internet, para poderem consultar os e-mails recebidos de forma offline. **Lembrem-se que – até um tempo atrás – o acesso à Internet era algo bastante raro e muitas pessoas não podiam ficar sem acesso aos**

seus e-mails quando não estivessem conectadas à Internet. Galera, a verdade é que o tempo foi passando e o POP3 foi se mostrando ineficiente em algumas situações.

#VamosPraticar#

(OBJETIVA / Prefeitura de Canoas-RS – 2023) O sistema de e-mail convencional é baseado na arquitetura cliente/servidor. As mensagens e os dados dos usuários que são utilizados para sua autenticação ficam no servidor. Os usuários utilizam uma interface (cliente) para criar, enviar e receber novas mensagens. Para um cliente ler as mensagens, pode ser usado o protocolo:

a) Simples File Transfer Protocol (SFTP)

b) Post Office Protocol (POP3).

c) Secure Shell (SSH).

d) Dynamic Host Configuration Protocol (DHCP).

e) Hypertext Transfer Protocol (HTTP).

Comentários: para um cliente ler as mensagens em um sistema de e-mail convencional baseado na arquitetura cliente/servidor, o protocolo apropriado é o POP3 (Letra B).

#VamosPraticar#

Ele não permite ao usuário organizar mensagens ou criar pastas no servidor; não permite que o usuário verifique parte do conteúdo da mensagem antes de fazer o download; possui problemas quando configurado em mais de um computador; etc. **Já o IMAP permite que você acesse todos os seus correios eletrônicos a qualquer momento.** Além disso, ele traz diversas funções adicionais. Vejamos...

E-Mail: IMAP

INTERNET MESSAGE ACCESS PROTOCOL (IMAP)
Protocolo da camada de aplicação responsável pelo acesso, gerenciamento e sincronização de e-mails armazenados em um servidor de e-mail. Ele permite ao usuário visualizar e manipular mensagens diretamente no servidor, além de sincronizar o estado das mensagens

(lido/não lido, marcado/não marcado) entre múltiplos dispositivos. Ele suporta criptografia via SSL/TLS e autenticação através de usuário e senha. Esse protocolo é mais flexível que o POP3, sendo ideal para usuários que acessam e-mail de múltiplos dispositivos. As mensagens geralmente permanecem no servidor, permitindo acesso a partir de qualquer dispositivo.

Um usuário pode verificar o cabeçalho de um e-mail antes de baixá-lo; pode procurar pelo conteúdo de um e-mail antes de baixá-lo; pode baixar parcialmente um e-mail – isso é útil se a largura de banda for limitada e o e-mail tiver conteúdos com grandes exigências de largura de banda; um usuário pode criar, eliminar ou renomear caixas de correio no servidor de e-mail; e pode criar uma hierarquia de caixas de correio em pastas para armazenamento de e-mails.

O IMAP é equivocadamente associado a webmails pelo caráter de repositório central que esses serviços oferecem ao permitir amplo acesso a e-mails (mobilidade). No entanto, navegadores (e consequentemente webmails) não suportam IMAP – eles utilizam o HTTP/HTTPS! **O IMAP possui uma versão mais segura chamada IMAPS (IMAP Secure). Nesse caso, ele utilizará a Porta 993 e, não, 143.** Vamos ver uma tabela comparativa:

Pop3	Imap
Post Office Protocol (Version 3)	Internet Message Access Protocol
Não recomendado para acesso em múltiplos dispositivos	Recomendado para acesso em múltiplos dispositivos
Não permite criar e organizar pastas no servidor	Permite criar e organizar pastas no servidor
Não permite verificar o cabeçalho antes de baixá-lo	Permite verificar o cabeçalho antes de baixá-lo
Modificações em um dispositivo não refletidas em outros	Modificações em um dispositivo refletidas em outros
Não permite baixar parcialmente um e-mail	Permite baixar parcialmente um e-mail
Por padrão, mensagens de e-mail são lidas offline	Por padrão, mensagens de e-mail são lidas online
Não permite múltiplas caixas postais	Permite múltiplas caixas postais
Porta 110	Porta 143

#VamosPraticar#

(FADENOR / Prefeitura de Nova Porteirinha-MG – 2023) Sobre os protocolos de e-mail, há um que permite que o usuário acesse o seu e-mail de diferentes dispositivos (smartphone, computador ou computador de um amigo), em qualquer lugar do mundo. Ao ler uma mensagem de e-mail usando-o, o usuário não a baixa ou armazena a mensagem em seu dispositivo; em vez disso, ele a lê a partir do serviço de e-mail. Ele só baixa uma mensagem quando se clica sobre ela para tal e os anexos não são baixados automaticamente. Dessa forma, o usuário pode verificar suas mensagens muito mais rapidamente do que através do protocolo POP, por exemplo. O trecho descrito refere-se ao protocolo:

a) TCP.

b) IMAP.

c) HTTP.

d) SMTP.

e) SSL.

Comentários: o trecho se refere ao IMAP, que é projetado para permitir o acesso a e-mails de diferentes dispositivos, em qualquer lugar, sem a necessidade de baixar ou armazenar as mensagens localmente. Ele permite que o usuário leia mensagens diretamente do serviço de e-mail, baixando-as apenas quando necessário. Este comportamento contrasta com o protocolo POP, que geralmente baixa todas as mensagens para o dispositivo local. Além disso, ele fornece uma experiência de e-mail mais rápida e flexível, especialmente útil para quem acessa e-mails de múltiplos dispositivos (Letra B).

#VamosPraticar#

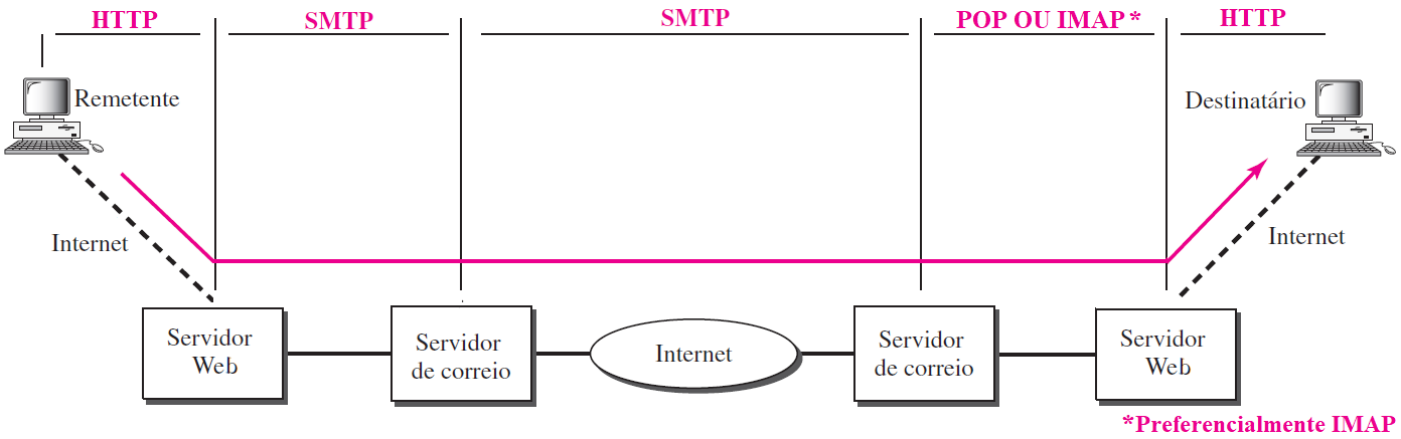
E-Mail: WebMail

webmail
Um webmail é um serviço de e-mail que pode ser acessado e usado através de um navegador da web, em vez de um cliente de e-mail dedicado. Ele funciona como uma

interface baseada na web para enviar, receber e gerenciar mensagens de e-mail (Ex: Gmail, Yahoo, Outlook, Hotmail, etc).

Agora vamos falar sobre um Webmail! **Trata-se de um sistema web que faz a interface com um serviço de e-mail hospedado em um Servidor Web!** *Armaria, professor... entendi foi nada!* Galera, quando vocês acessam a página do Estratégia Concursos, vocês estão acessando – por meio de um browser – uma página que está hospedada (armazenada) em uma máquina especializada chamada Servidor Web. Ocorre de maneira semelhante com e-mail...

Quando vocês acessam – por meio de um navegador – um serviço de e-mail, temos um... webmail! **É como se o cliente de e-mail apresentado no esquema anterior estivesse hospedado em um servidor web e você utilizasse um browser para acessá-lo.** Logo, a comunicação entre a máquina do remetente e o servidor web de origem se dá por meio do HTTP! Ao final, para recuperar o e-mail do servidor web para a máquina do destinatário também se utiliza o HTTP.



Algumas questões não primam pelo rigor técnico e acabam omitindo o servidor web e tratando ambos – servidor web e servidor de correio eletrônico – apenas como servidor de correio eletrônico.

CARACTERÍSTICAS DE WEBMAIL	DESCRIÇÃO
Acessibilidade	Webmails podem ser acessados de qualquer dispositivo com uma conexão à internet e um navegador web, oferecendo grande conveniência e mobilidade.
Não querer instalação de software	Ao contrário dos clientes de e-mail que requerem instalação, como Microsoft Outlook ou Mozilla Thunderbird, o webmail opera inteiramente no navegador.
Armazenamento na nuvem	As mensagens de e-mail são armazenadas no servidor do provedor de e-mail, não no dispositivo local. Isso facilita o acesso a e-mails de diferentes dispositivos.

Interface do usuário	Webmails geralmente têm interfaces de usuário ricas, semelhantes a aplicações desktop, com recursos como arrastar e soltar, pastas, e ferramentas de busca avançada.
Segurança e manutenção	A segurança e a atualização de software são gerenciadas pelo provedor do serviço, reduzindo a necessidade de manutenção por parte do usuário.
Integração com outros serviços	Muitos webmails são integrados com outros serviços online, como calendários, gerenciamento de contatos, armazenamento em nuvem e aplicações de escritório.

#VamosPraticar#

(OBJETIVA / Prefeitura de Lavras do Sul-RS – 2023) O correio eletrônico (E-mail ou Electronic Mail) é um dos serviços mais utilizados na Internet. Considerando-se os principais conceitos de correios eletrônicos, assinalar a alternativa que preenche as lacunas abaixo CORRETAMENTE:

Um _____ é um sistema que permite aos seus usuários acessar suas mensagens utilizando apenas um navegador Internet, sem que haja a necessidade de se instalar e configurar programas clientes de e-mail. Um _____ pode ser uma solução para empresas que desejam permitir que seus funcionários acessem suas contas de e-mail fora da empresa.

a) webmail

b) spool

c) mail transport agent

d) IMAP

Comentários: a questão trata do Webmail, responsável por oferecer acesso a e-mails por meio de um navegador web, sem a necessidade de instalar um cliente de e-mail dedicado – ideal para acesso remoto e uso em diferentes dispositivos (Letra A).

#VamosPraticar#

E-Mail: MIME

Multipurpose Internet Mail Extensions (mime)
Trata-se de um padrão importante no contexto do correio eletrônico. Ele expande as capacidades do e-mail original, que era limitado a textos em formato ASCII, permitindo a inclusão de uma variedade de tipos de conteúdo. Ele é essencial para a funcionalidade moderna do e-mail, permitindo uma rica variedade de conteúdos e formatos de arquivo a serem compartilhados por meio deste meio de comunicação.

Para finalizar de vez essa parte de correio eletrônico, vamos falar rapidamente sobre **MIME**! O correio eletrônico possui uma estrutura simples, porém isso tem um preço. Ele, por exemplo, possui certas limitações no formato de envio de algumas mensagens. Originalmente, ele não pode ser utilizado para criar mensagens em idiomas que não são suportados por caracteres ASCII de 7 bits (como francês, alemão, hebraico, russo, chinês e japonês).

Da mesma forma, ele não pode ser usado para transmitir arquivos binários ou dados no formato de fotos, áudio ou vídeo. *Professor, mas eu já enviei e-mail com todos esses formatos!* Se você já fez isso, agradeça ao MIME! **Ele é um protocolo complementar ao SMTP que possibilita que dados em diferentes formatos sejam enviados por e-mail.** Podemos imaginar o MIME como um conjunto de funções de software que convertem dados não-ASCII (fluxos de bits) em dados ASCII e vice-versa.

Em outras palavras, ele é um recurso, formato ou extensão utilizado para formatação de mensagens que facilita o envio de mensagens e permite o envio de arquivos de diferentes tipos (imagem, áudio, vídeo, documento, executável, etc) em um e-mail. Ele também possui uma versão mais segura – que permite a criptografia e assinatura dos dados – chamada S/MIME. Isso não costuma cair com frequência, mas é bem simples de entender...

CARACTERÍSTICAS DE mime	DESCRIÇÃO
Tipos de conteúdo	Permite que e-mails incluam diferentes tipos de conteúdo, como texto em diferentes codificações de caracteres, imagens, vídeos, arquivos de áudio e documentos anexados.
Anexos de e-mail	Permite anexar arquivos a e-mails. Isso é possível devido à maneira como o MIME codifica esses arquivos para serem compatíveis com o sistema de e-mail.

Codificação de conteúdo	Codifica dados binários para formatos que são compatíveis com os padrões de e-mail baseados em texto.
Extensibilidade	É projetado para ser extensível, com a capacidade de suportar novos tipos de mídia conforme são desenvolvidos.
Padrão de internet	Tornou-se um padrão de fato para mensagens de e-mail na Internet, sendo amplamente adotado em quase todos os sistemas modernos de e-mail.
Cabeçalhos mime	Informações são incluídas nos cabeçalhos das mensagens de e-mail, permitindo que clientes de e-mail saibam como processar o conteúdo recebido.

#VamosPraticar#

(IBADE / Prefeitura de Manaus – 2018) Um formato básico de mensagens transmitidas e enviadas, que é utilizado em softwares de correio eletrônico, é o:

a) MIME

b) FTP

c) URL

d) ARPNET

Comentários: o formato básico de mensagens transmitidas e enviadas em softwares de correio eletrônico é conhecido como MIME (Letra A).

#VamosPraticar#

Protocolo DHCP

INCIDÊNCIA EM PROVA: BAIXA

Dynamic host configuration protocol (dhcp)
Protocolo da camada de aplicação responsável por atribuir automaticamente endereços IP e outras configurações de rede a dispositivos em uma rede. Ele funciona com um modelo cliente-servidor em que o Servidor DHCP atribui IPs dinamicamente aos clientes da rede e suporta alocação dinâmica, alocação automática e alocação estática de endereços IP. O DHCP simplifica o gerenciamento de endereços IP (especialmente em redes grandes), sendo amplamente utilizado em redes domésticas, corporativas e públicas para simplificar a configuração de rede.

O DHCP (Dynamic Host Configuration Protocol) é um protocolo cliente/servidor da camada de aplicação que permite a alocação estática ou dinâmica de endereços lógicos de forma manual ou automática. *O que é um endereço lógico?* É o Endereço IP! Não confundam com o endereço físico (Endereço MAC). Em contraste com o endereço físico, que está sempre associado a um hardware e jamais pode mudar, o endereço lógico pode mudar sem problemas.

Todo dispositivo na internet precisa ter um endereço lógico único. *Você pode simplesmente chutar algum endereço lógico aleatório para acessar à internet?* Não, diversos endereços lógicos já estão sendo utilizados, outros possuem proprietários, outros são reservados, etc. Você precisa contratar um endereço lógico através de algum Provedor de Serviço de Internet (Ex: Net, Claro, Vivo, etc). **No entanto, é importante notar que existem dois tipos de Endereço IP: Estático e Dinâmico.**

Como o próprio nome sugere, o endereço estático é fixo e somente pode ser modificado manualmente pelo próprio provedor de internet ou pelo administrador da rede. Ele geralmente é atribuído aos servidores, visto que se espera que esse endereço não seja modificado. *Galera, já pensaram se o endereço lógico do Estratégia Concursos fosse dinâmico?* Todo dia você teria que descobrir qual era o novo endereço para acessar a página e ler os livros ou assistir aos vídeos.

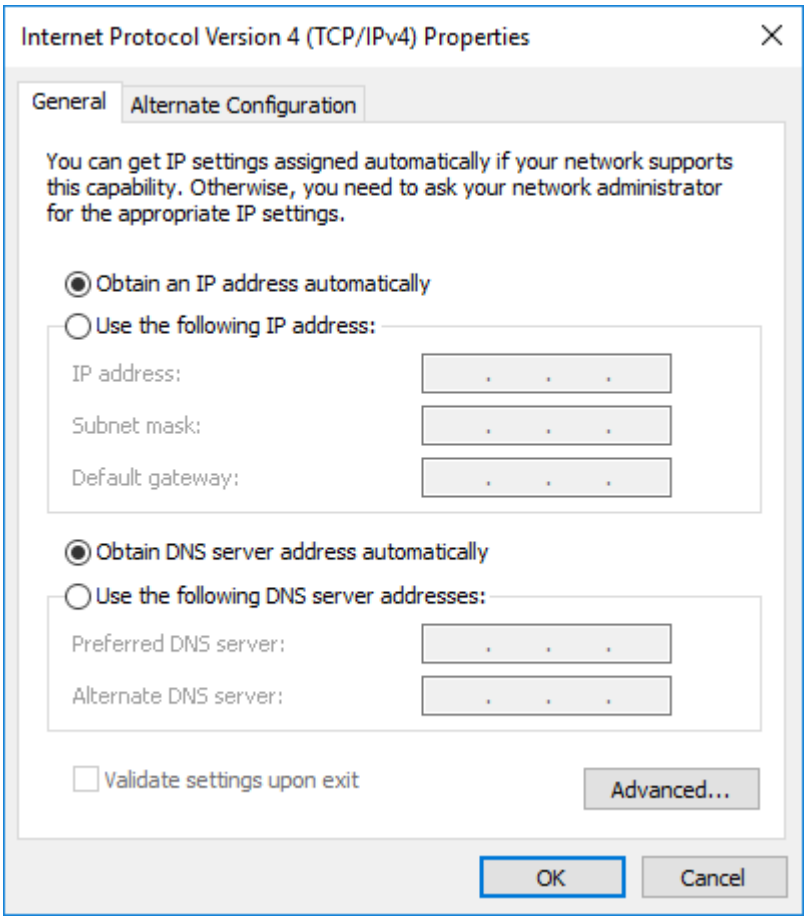
Hoje é muito raro encontrar usuários que possuam endereços estáticos, já que a maioria das operadoras preferiram adotar o sistema de endereços dinâmicos para usuários domésticos, por ele ser mais seguro e eficiente. **Já o endereço dinâmico é alocado em tempo de conexão, sendo configurado automaticamente por meio do protocolo DHCP.** Ele geralmente é atribuído aos clientes, visto que seu endereço poder ser modificado a cada nova conexão.

É o padrão ideal para uso doméstico, já que não requer equipamentos de melhor performance, é mais barato e não depende de conhecimentos um pouco mais avançados para configuração e manutenção. Por falar nisso, a configuração de uma rede pode ser feita de maneira manual. **Dessa forma, a configuração tem que ser feita máquina a máquina a partir das propriedades de conexão local.** *Já imaginaram uma rede com 500 computadores?*

Essa configuração pode ser trabalhosa, exigindo uma equipe técnica e ocasionando erros importantes quando temos uma rede com muitos computadores para configurar. No entanto, essa configuração também pode ser feita de forma automática. **Nesse caso, utiliza-se um**

servidor para obtenção de um Endereço IP. O nome desse servidor capaz de encontrar um endereço IP é Servidor DHCP – é importante relembrar que se trata de um protocolo cliente/servidor...

Antigamente, era necessário ligar no provedor de serviço toda vez que você quisesse acessar à internet para obter informações necessárias para a configuração da rede. Você ligava e perguntava qual era o endereço lógico, qual era a máscara de sub-rede, qual era o gateway padrão, qual era o endereço do Servidor DNS, etc. **Hoje em dia, basta utilizar um Servidor DHCP – ele será responsável por fazer toda essa configuração automaticamente.**



O Servidor DHCP recupera essas informações, configura a rede e aloca um endereço lógico dinâmico para a máquina cliente. Ao terminar a conexão, ele desaloca o endereço lógico para permitir que ele possa ser utilizado por outro cliente em uma nova conexão. **Logo, esse protocolo é capaz de atribuir uma alocação dinâmica de endereços lógicos (entre outras configurações) de forma automática.**

#VamosPraticar#

(ACCESS / CRBIO6 – 2023) No que diz respeito às redes de computadores, um serviço implementado nos roteadores tem por finalidade distribuir e atribuir um endereço IP aos celulares, microcomputadores e notebooks, de forma lógica, automática e dinâmica, viabilizando o acesso wifi desses dispositivos à internet. Esse serviço é conhecido pela sigla:

a) DNS.

b) SSH.

c) DHCP.

d) HTTP.

Comentários: DHCP é um protocolo que permite aos roteadores e outros dispositivos de rede atribuir automaticamente endereços IP e outras configurações de rede a dispositivos como celulares, microcomputadores e notebooks, facilitando sua conexão à internet (Letra C).

(SELECON / Prefeitura de Cuiabá-MT – 2018) Atualmente, é comum a configuração de um recurso nos roteadores padrão IEE-802.11/n/ac para concessão de acesso à internet em microcomputadores e dispositivos móveis, por meio da atribuição dinâmica de endereços IP. Este recurso utiliza um modelo cliente-servidor, que faz a gestão centralizada dos endereços IP usados na rede. O cliente consiste em um dispositivo de rede que tem a capacidade de adquirir as configurações do TCP/IP do servidor. Graças a este recurso, os dispositivos da rede recebem as configurações do servidor central e, assim, o utilizador não precisa configurar os endereços manualmente.

Esse recurso é conhecido pela seguinte sigla:

a) DHCP

b) HPFS

c) DNS

d) NFS

Comentários: a questão trata do DHCP, protocolo responsável por essa gestão centralizada dos endereços IP em uma rede, permitindo que os dispositivos clientes recebam automaticamente configurações de TCP/IP de um servidor central, sem a necessidade de configurações manuais (Letra A).

#VamosPraticar#

Protocolo DNS

INCIDÊNCIA EM PROVA: ALTÍSSIMA
Domain Name System (DNS)
Protocolo da camada de aplicação responsável por traduzir (também chamado de resolver) nomes de domínio legíveis por humanos para Endereços IP. Ele funciona em um modelo de consulta e resposta, sendo estruturado de maneira hierárquica com vários níveis de Servidores DNS. Esse protocolo armazena as respostas recentes para reduzir o tempo de resposta e o tráfego na rede, incluindo extensões de segurança para proteger contra ataques. O DNS é essencial para a navegação na internet, permitindo o uso de URLs em vez de endereços IP numéricos.

D	N	S
DÁ	NOME AO	SITE

DNS: Funcionamento

Galera, quantos números vocês sabem decorados? Eu, por exemplo, tenho uma péssima memória! Eu sei meu Nº de CPF, Nº de RG, Nº de Conta Bancária e Nº de Telefone. Fora isso, eu já começo a ter dificuldades de lembrar. Nós sabemos que os computadores na Internet são identificados utilizando endereços IP (Exemplo: 192.168.10.15). **Uma vez que é mais fácil decorar nomes que números, foi criado um sistema capaz de traduzir números em nomes e vice-versa**.

Vamos fazer mais um teste! Dessa vez, eu quero que vocês abram um navegador web qualquer, digitem **216.58.211.14** e vejam o que acontece! **Pois é, abrirá a página do Google!** *Professor, como isso é possível?* Galera, toda página web está armazenada em algum servidor e nós já sabemos que todo dispositivo na internet precisa ter um endereço lógico exclusivo. Logo, um servidor também precisa de um endereço para ser acessado.

O servidor que armazena o Google tem o endereço lógico 216.58.211.14. *Agora vocês já imaginaram se nós tivéssemos que decorar todos os endereços IP de todos os sites que nós acessamos diariamente?* Seria completamente inviável! Para resolver esse problema, surgiu o Domain Name System (DNS). **Trata-se de um protocolo cliente/servidor da camada de aplicação responsável por atribuir endereços léxicos aos recursos da rede** – ele é como uma agenda de contatos da Internet!

Professor, falou difícil agora! Galera, endereço léxicos são aqueles formados por palavras ou vocábulos de um idioma, em vez de um número. Em outras palavras, ele busca transformar endereços numéricos em nomes amigáveis, mais compreensíveis para humanos e mais fáceis

de memorizar. *O que é mais fácil de decorar: 216.58.211.14 ou Google.com* [20]? Pois é! Notem que, apesar de ser mais fácil para **você** memorizar, o **computador** entende apenas Endereço IP.

Imaginem que um dia você sai de uma balada de madrugada, chama um taxi e simplesmente diz ao motorista: "*Parceiro, me leva na casa do João*"! Ué, galera... o taxista lá sabe quem é João? Taxista conhece endereços e, não, nomes de pessoas. **Nessa analogia, o taxista seria o seu navegador – ele só reconhece endereços e, não, nomes de pessoas**. *Professor, como o DNS consegue fazer essa tradução de nome para endereço e vice-versa?*

Vocês sabem decorados todos os números de telefone armazenados no smartphone? Eu duvido! Quando vocês querem ligar para alguém, vocês procuram o nome de um contato e o celular disca o número armazenado. E se vocês, por algum acaso, souberem o número, ele faz o caminho inverso e identifica o nome. O DNS funciona exatamente como a agenda telefônica de um smartphone. **A tabela seguinte mostra a correspondência entre URL e Endereço IP:**

DNS (DOMAIN NAME SYSTEM)	
URL	**IP**
www.google.com [21]	216.58.211.14

DNS: URL

Antes de prosseguir, vamos entender o que é uma URL (*Uniform Resouce Locator*)! **Trata-se do endereço de um recurso em uma rede de computadores.** Todo recurso computacional (página web, arquivo, servidor, impressora, computador, documento, entre outros) deve possuir um endereço para que possa ser localizada. Ela oferece uma maneira uniforme e padronizada de localizar recursos na rede. Uma URL é formada pela seguinte estrutura:

URL - Sintaxe abstrata
protocolo://ip-ou-domínio:porta/caminho/recurso

Componentes	DESCRIÇÃO
Protocolo	Também chamado de esquema, trata-se do protocolo utilizado para acessar um recurso.
ip	Número de IP do Servidor (Host) que hospeda um recurso.

DOmínio	Nome do Domínio do Servidor (Host) que hospeda um recurso.
PORTA	Ponto lógico que permite criar uma conexão em um processo.
Caminho	Estrutura de diretórios dentro do servidor que armazena um recurso.
recurso	Componente físico ou lógico disponível em um sistema computacional.

Pessoal, os componentes de um endereço funcionam para ajudar a encontrar o recurso desejado. Vamos pensar em um endereço fictício: SQN 115 Bloco A Apt 208 – Asa Norte – Brasília/DF (sim, os endereços em Brasília são meio malucos). Eu estou dizendo que – para encontrar esse endereço – você deve ir até o Distrito Federal, localizar Brasília, se deslocar até a Asa Norte, seguir até a SQN 115, procurar o Bloco A e chegar no Apt 208.

A URL é o endereço virtual de um recurso em uma rede, logo ela está informando que para encontrar o recurso desejado, você deve utilizar um determinado protocolo, informar o endereço lógico ou nome do domínio para encontrar o servidor, depois procurar em uma porta específica, seguir um caminho nos diretórios no disco que armazena esse recurso até finalmente encontrá-lo. Então vamos ver um exemplo:

https://www.estrategiaconcursos.com.br/app/dashboard/cursos/aulas/aula1.pdf [22]

Componentes	DESCRIÇÃO
Protocolo	https
domínio	estrategiaconcursos.com.br [23] (www é apenas um prefixo que pode ser omitido)
PORTA	443 (apesar de ter sido omitida, essa é a porta padrão desse protocolo)
Caminho	/app/dashboard/cursos/aulas
recurso	Aula1.pdf

Existe uma confusão entre URL e Domínio! Observem que – se eu modifico o nome do recurso da URL anterior para "*Aula2.pdf*", eu terei uma URL diferente, no entanto o domínio permanecerá o mesmo! Pessoal, nós vimos na página anterior a sintaxe abstrata de uma URL! *Por que dizemos que se trata de uma sintaxe abstrata?* **Porque a sintaxe completa pode conter vários outros componentes como apresentado abaixo:**

URL – sintaxe completa
protocolo://nome-de-usuário@ip-ou-domínio:porta/caminho/recurso?query#fragmento

Note que temos três componentes extras: o Nome de Usuário é um subcomponente utilizado para indicar o usuário de um determinado servidor; a Query String (ou consulta) são parâmetros e valores usados para realizar uma consulta ou pesquisa; e o Fragmento é parte de um documento ou recurso específico dentro do recurso principal. Note que alguns componentes podem ser adicionados à URL para fornecer informações adicionais ou especificar determinadas partes do recurso.

#VamosPraticar#

(IDIB / Ministério da Economia – 2021) Assinale a alternativa com a correta complementação: URL, Universal Resource Locator, é o nome dado a um:

a) endereço Web utilizado para acessar e identificar páginas eletrônicas na Web.

b) protocolo de rede para acesso às páginas eletrônicas.

c) aplicativo utilizado para buscar as páginas eletrônicas na Web.

d) endereço de e-mail utilizado para acessar e identificar a caixa postal eletrônica dos usuários.

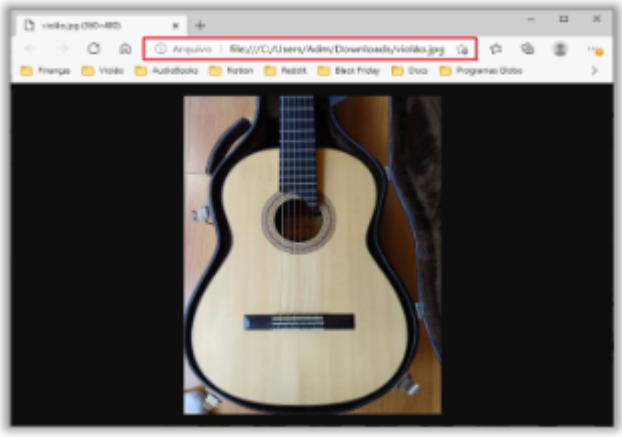
e) aplicativo que identifica os arquivos criados com o navegador Mozilla.

Comentários: (a) Correto. Uma URL é um endereço na web que é usado para acessar e identificar recursos na Internet, incluindo páginas eletrônicas; (b) Errado. Uma URL não é um protocolo de rede; ela pode incluir um protocolo de rede em sua estrutura (como HTTP ou HTTPS), mas a URL em si é um endereço que aponta para um recurso na web; (c) Errado. Uma URL não é um aplicativo; é um endereço que pode ser usado em um navegador web (ou outro cliente de rede) para acessar páginas eletrônicas; (d) Errado. Uma URL é usada para localizar recursos na Internet, não para identificar endereços de e-mail. Endereços de e-mail têm um formato diferente e servem a um propósito distinto; (e) Errado. Uma URL não é um aplicativo e não está limitada a identificar arquivos criados com qualquer navegador específico, incluindo o Mozilla. Ela é um endereço universal usado para acessar recursos na Internet (Letra A).

#VamosPraticar#

DNS: Esquemas

Algumas observações importantes: os principais componentes em uma URL são o Protocolo e o Domínio – todos os outros costumam ser omitidos com alguma frequência. Além disso, os protocolos ou esquemas mais comuns que são suportados em uma URL são: **HTTP, HTTPS, FTP, FILE e MAILTO**. Os três primeiros protocolos ainda serão vistos nessa aula, já os dois últimos esquemas nós veremos agora...



O FILE é um esquema tipicamente utilizado para indicar que se trata de um recurso local, isto é, está localizado dentro do próprio computador do usuário. Se você abrir na aba do seu navegador algum recurso localizado dentro do seu próprio computador, você verá que na barra de endereços aparecerá uma URL iniciada pelo esquema FILE. **Na imagem ao lado, eu abri uma foto do meu violão dentro do browser, logo o esquema da URL contida na barra de endereços começa pelo esquema file://.** *Entendido?*

#VamosPraticar#

(CESPE / Polícia Federal – 2018) URL (Uniform Resource Locator) é um endereço virtual utilizado na web que pode estar associado a um sítio, um computador ou a um arquivo.

Comentários: URL é o endereço de um recurso na rede! *É um endereço virtual?* Sim. *Utilizado na web?* Sim. *Pode estar associado a um sítio, um computador ou arquivo?* Sim, o recurso pode ser sítio, página web, computador, arquivo, documento, etc (Correto).

#VamosPraticar#

Já o esquema MAILTO é utilizado para escrever um e-mail para um destinatário específico. Observem na imagem abaixo que eu inseri a URL: *mailto:// professordiegocarvalho@gmail.com* [24] [25] (inclusive, ele permite omitir o // e também inserir o

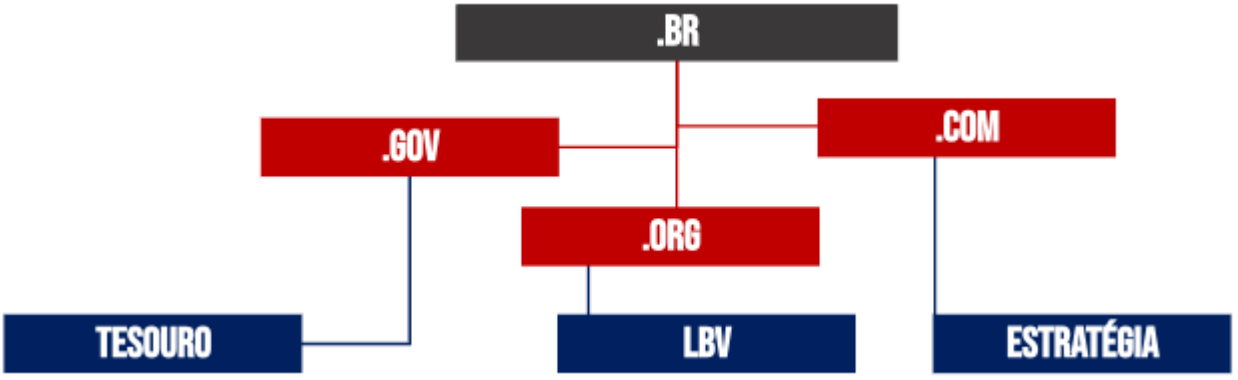
assunto). Ao pressionar a tecla ENTER, uma janela de Nova Mensagem é aberta no meu cliente de correio eletrônico padrão já com o endereço de destinatário preenchido de acordo com que o que constava na URL.

Também é importante destacar que – como todos os serviços disponíveis na *Internet* – o correio eletrônico é disponibilizado através de servidores e, para acessá-los, o DNS efetua as conversões de endereços para que os servidores sejam localizados. Notem nos exemplos abaixo que algumas URLs possuem porta, outros não; algumas possuem protocolo, outros esquema, outros nenhum; algumas possuem caminho, outros não; etc...

Exemplos de url	
www.estrategiaconcursos.com.br [26]	mailto:diego@carvalho?subject=informatica [27]
http://www.estrategiaconcursos.com.br [28]	https://www.estrategiaconcursos.com.br/professores [29]
mailto:// [30]contato@diegocarvalho.com.br [31]	ftp://admin@diegocarvalho.com.br [32]
http://www.estrategiaconcursos.com.br:80 [33]	mailto:professordiegocarvalho@gmail.com [34]

DNS: Hierarquia

O domínio é o principal componente de uma URL e, por isso, dizemos que o DNS traduz, transforma, resolve um Nome/Domínio em um Endereço IP e vice-versa. Agora vamos falar mais detalhadamente sobre domínios. **O DNS é um protocolo cliente/servidor que apresenta uma estrutura hierárquica e distribuída, em que seu espaço de nomes é dividido em vários servidores de domínio baseado em níveis.** Vejam a imagem seguinte...



Diego, o que é um espaço de nomes? Para evitar ambiguidades, os nomes atribuídos às máquinas devem ser cuidadosamente selecionados a partir de um espaço de nomes – que nada mais é que um conjunto organizado de possíveis nomes. **Em outras palavras, os nomes**

devem ser exclusivos, uma vez que os endereços IP também o são. A entidade que controla o registro e manutenção de domínios em nível global é chamada de ICANN.

Essa entidade define que o domínio .br pertence ao Brasil [35]; o domínio .pt pertence à Portugal; o domínio .jp pertence ao Japão; o domínio .es pertence à Espanha; entre outros. **Já em nível nacional, existe uma outra entidade responsável pelo registro e manutenção de domínios brasileiros chamada Registro.br** [36]**.** Caso algum dia vocês queiram adquirir e registrar um domínio próprio, vocês provavelmente terão que acessar a página seguinte:

www.registro.br [37]

Professor, eu não tenho grana para isso não! Galera, fiquem tranquilos porque é bem baratinho. Em um plano de 10 anos, custaria pouco mais de R$3/Mês.

Além disso, existem algumas subcategorias de domínio **.br**. *Como assim, professor?* Se você exerce uma atividade comercial, você poderá ter um domínio **.com.br** [38]; se você possui uma organização não-governamental sem fins lucrativos, você poderá ter um domínio **.org.br** [39]. Algumas categorias possuem ainda restrições adicionais por serem direcionadas a empresas de setores específicos, sendo necessária comprovação por meio de envio de documentos. Vejamos...

Pessoas Jurídicas

COM RESTRIÇÃO	
AM.BR	Empresas de radiodifusão sonora
COOP.BR	Cooperativas
FM.BR	Empresas de radiodifusão sonora
G12.BR	Instituições de ensino de primeiro e segundo grau
GOV.BR	Instituições do governo federal
MIL.BR	Forças Armadas Brasileiras
ORG.BR	Instituições não governamentais sem fins lucrativos
PSI.BR	Provedores de serviço Internet
DNSSEC OBRIGATÓRIO	
B.BR	Bancos
DEF.BR	Defensorias Públicas
JUS.BR	Instituições do Poder Judiciário
LEG.BR	Instituições do Poder Legislativo
MP.BR	Instituições do Ministério Público

Genéricos

Para pessoas físicas ou jurídicas

ART.BR	Artes: música, pintura, folclore
COM.BR	Atividades comerciais
ECO.BR	Atividades com foco eco-ambiental
EMP.BR	Pequenas e micro-empresas
NET.BR	Atividades comerciais
ONG.BR	Atividades não governamentais individuais ou associativas

Universidades

EDU.BR	Instituições de ensino superior

Pessoas Físicas

BLOG.BR	Web logs
FLOG.BR	Foto logs
NOM.BR	Pessoas Físicas
VLOG.BR	Vídeo logs
WIKI.BR	Páginas do tipo 'wiki'

Existem algumas regras que devem ser observadas em um nome de domínio registrado no Registro.br [40]: (1) deve possuir entre 2 e 26 caracteres, não incluindo a categoria. Logo, o domínio *www.x.com.br* [41] é inválido porque possui apenas 1 caractere; (2) deve ser composta por caracteres alfanuméricos. Logo, o domínio *www.123.com.br* [42] é inválido porque não contém letras; (3) não pode começar ou terminar com hífen, mas pode ter acentuação e cedilha desde 2008.

Domínio **estrategiaconcursos.com.br**

TITULAR	ESTRATÉGIA CONCURSOS LTDA
DOCUMENTO	13.877.842/0001-78
RESPONSÁVEL	Heber Carvalho
PAÍS	BR
CONTATO DO TITULAR	ESCON22
CONTATO ADMINISTRATIVO	HFACA2
CONTATO TÉCNICO	AMJ216
CONTATO COBRANÇA	HFACA2
SERVIDOR DNS	alan.ns.cloudflare.com
SERVIDOR DNS	emily.ns.cloudflare.com
SACI	Sim
CRIADO	29/04/2011 #8227683
EXPIRAÇÃO	29/04/2027
ALTERADO	11/12/2018
STATUS	Publicado

Por fim, vamos falar rapidinho sobre o Whois! **Trata-se de um serviço que permite consultar informações sobre os responsáveis por domínios e blocos de IP registrados na Internet.** *Como assim, Diego?* Imagine que houve uma tentativa de invasão à rede de um órgão, mas que foi impedida por um firewall, que salvou o endereço IP da tentativa de invasão.

Qual seria uma atitude recomendável do administrador dessa rede? Bem, ele poderia consultar um Servidor Whois para tentar identificar informações úteis sobre o invasor. Galera, esse é apenas um cenário, mas você – sim, você mesmo – pode consultar um Servidor Whois em busca de informações sobre qualquer Domínio ou Endereço IP.

Vamos tentar descobrir informações sobre o domínio ***www.estrategiaconcursos.com.br*** [43]. Como se trata de um domínio brasileiro, basta acessar o **registro.br** [44] em:

https://registro.br/tecnologia/ferramentas/whois [45]

Vejam que são exibidos diversos dados sobre esse domínio, tal como: Titular, Documento, Responsável, País, Contatos, Servidor DNS, Data de Criação, Data de Expiração, entre outros. Vejam que o domínio foi registrado em 29 de abril de 2011 pelo Prof. Heber Carvalho – um dos sócios-fundadores do Estratégia Concursos. Para um domínio **.com**, pode-se utilizar o serviço ***www.who.is*** [46] para pesquisas.

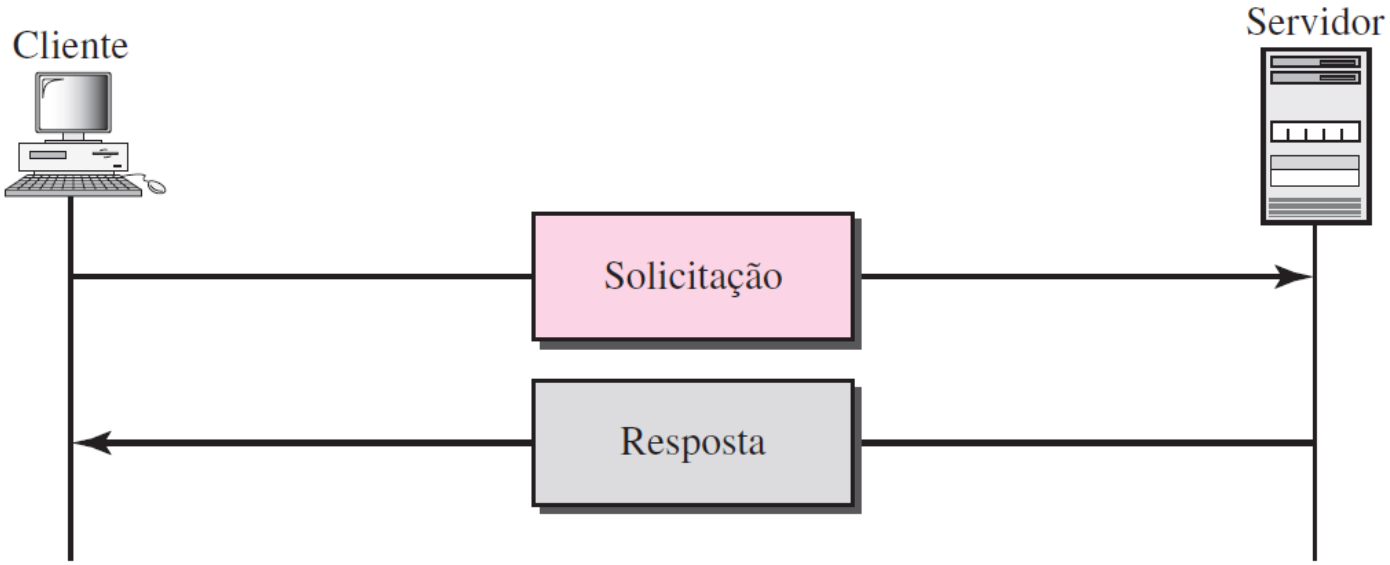
Protocolos Web

INCIDÊNCIA EM PROVA: Altíssima

Web: HTTP

Hypertext transfer protocol (http)
Protocolo da camada de aplicação utilizado para carregar páginas da web, enviar formulários, realizar transações online, obter recursos, entre outros. Trata-se de um protocolo baseado em um modelo de requisição-resposta entre um cliente (Navegador Web) e um servidor (Servidor Web): mensagens enviadas pelo cliente são chamadas de solicitações ou requisições (Requests) e as mensagens enviadas pelo servidor são chamadas de respostas (Responses).

O HTTP (*HyperText Transfer Protocol*) é um protocolo cliente/servidor da camada de aplicação utilizado por programas de navegação (browsers) para acessar dados na web. Em português, seria traduzido como Protocolo de Transferência de Hipertexto, sendo responsável pela transferência, formatação e apresentação de páginas web com conteúdo multimídia (textos, áudio, imagens, vídeos, etc) entre um servidor e um cliente na Internet.



A imagem anterior ilustra uma transação típica entre um Cliente HTTP e um Servidor HTTP. O cliente inicializa uma transação enviando uma mensagem de solicitação. O servidor responde enviando uma mensagem de resposta. *Como assim, Diego?* Galera, toda página web está armazenada em um servidor web. Logo, quando você acessa qualquer página pelo navegador, você está fazendo uma solicitação ao servidor para acessar aquela página.

Se você conseguir acessá-la, significa que o servidor web autorizou e te devolveu como resposta a página que você desejava acessar. **Por falar em servidor web, esse é o nome dado ao servidor que hospeda ou armazena páginas ou recursos web** – assim como o servidor que armazena e-mails é chamado de servidor de e-mail. Prosseguindo... toda solicitação ou requisição a um servidor web retorna um código de status de três dígitos e divididos em cinco categorias:

CÓDIGO	CATEGORIA	SIGNIFICADO

1XX	INFORMAÇÃO	100 significa que o servidor concorda em atender à requisição.
2XX	SUCESSO	200 significa que a requisição foi bem-sucedida e 204 significa que a página está sem conteúdo.
3XX	REDIRECIONAMENTO	301 significa que a página foi movida e 304 significa que a página em cache ainda é válida.
4XX	ERRO DO CLIENTE	403 significa que a página é proibida e 404 significa que a página não foi encontrada.
5XX	ERRO DO SERVIDOR	500 significa que houve um erro interno e 503 significa que você deve tentar novamente mais tarde.

Professor, há como explicar melhor o que você quis dizer? Claro que sim! Façam um teste: abram um navegador e digitem: www.estrategiaconcursos.com.br/euamopinkfloyd [47].

Home | Cursos Online | Professores | Depoimentos | Coaching | Blog | Aulas ao vivo

Home » Erro 404 - Mapa do Site

ERRO 404 - PÁGINA NÃO ENCONTRADA

A página que você procura não foi encontrada.

Vocês viram que retornou um erro? Pois é, Erro 404! Esse erro é da categoria Erro do Cliente e significa que uma determinada página não foi encontrada. *Por que, professor?* Cara, essa página não foi encontrada basicamente porque ela não existe – eu acabei de inventar apenas para mostrar um código de retorno! **Esse código sempre existirá para qualquer requisição, mas nem sempre será exibido para os usuários (se houve sucesso, não faz sentido exibir).**

5xx Server Error: entenda o erro que tirou WhatsApp, Facebook e Instagram do ar

Erro de servidor faz com que usuários não possam acessar os serviços das plataformas do Facebook nesta segunda-feira (4)

Vocês se lembram quando o Whatsapp, Instagram e Facebook caíram por um dia inteiro? Ao tentar acessar essas páginas, aparecia um **ERRO 5XX**. Ele significa que o problema está sendo ocasionado por uma falha nos servidores. Na prática, ele ocorre quando o servidor (computador central) não consegue completar a solicitação do usuário e, por isso, não tem como exibir a informação desejada. Há, inclusive um site que ajuda a verificar se um servidor está fora do ar:

https://www.downdetector.com [48]

#VamosPraticar#

(AVANÇA / Prefeitura de Louveira-SP – 2021) O que descreve a mensagem HTTP 404?

a) problema de resolução do DNS.

b) problema de vírus no computador.

c) página solicitada não foi encontrada pelo servidor.

d) problema de segurança no navegador.

e) problema de endereçamento UJG.

Comentários: (a) Errado. Problemas de resolução do DNS normalmente resultam em erros diferentes do Erro 404; (b) Errado. presença de vírus no computador pode causar vários problemas, mas o erro HTTP 404 não está diretamente relacionado a vírus; (c) Correto. Essa mensagem é exibida quando uma página ou recurso não pode ser encontrado no servidor – isto pode acontecer se a página foi removida, mudou de nome, ou nunca existiu; (d) Errado. Problemas de segurança no navegador são normalmente indicados por mensagens de erro diferentes, relacionadas a questões de certificados, por exemplo; (e) Errado. essa mensagem não é reconhecida no contexto de erros HTTP (Letra C).

#VamosPraticar#

HTTP é um **protocolo** para transferência ou acesso de hipertexto e HTML é uma **linguagem** para criação de páginas web. **HTTP** é **Protocolo** e **HTML** é **Linguagem**.

#VamosPraticar#

(QUADRIX / CRA-PE – 2023) O HTTP (HyperText Transfer Protocol) é o protocolo que permite ao usuário acessar diversos sites na web. Ele tem a função de transferir páginas escritas em HTML (HyperText Markup Language) para o navegador instalado no computador do usuário.

Comentários: HTTP é um protocolo de comunicação na Internet que é utilizado para a transferência de dados, principalmente páginas web escritas em HTML (HyperText Markup Language). Este protocolo define como mensagens são formatadas e transmitidas, e como

servidores e navegadores da web devem responder a essas mensagens. Quando um usuário acessa um site, o navegador envia uma solicitação HTTP ao servidor do site, que responde enviando os arquivos da página web, normalmente em HTML, para serem renderizados e exibidos pelo navegador (Correto).

(IFTO / IFTO – 2018) Os protocolos de comunicação, em redes de computadores, são o conjunto de regras que governam a interação entre sistemas de computadores distribuídos em rede. Os protocolos são usados para permitir a comunicação entre dois ou mais computadores. Os navegadores de internet utilizam um protocolo que é a base de comunicação de dados da world wide web, específico para a transferência e apresentação de páginas com conteúdo multimídia (informações de textos, áudio, imagens e vídeos). Assinale a opção correta que identifica o protocolo usado pelos browsers que permitem os usuários a navegar na internet.

a) File Transfer Protocol (FTP)

b) Internet Message Access Protocol (IMAP)

c) Simple Mail Transfer Protocol (SMTP)

d) Post Office Protocol (POP)

e) HyperText Transfer Protocol (HTTP)

Comentários: HTTP é o protocolo de comunicação usado para transferir páginas da web entre navegadores e servidores web. Ele é responsável por definir como os navegadores solicitam páginas da web aos servidores web e como os servidores web respondem às solicitações dos navegadores. Os outros protocolos listados são usados para outras finalidades. O FTP é usado para transferir arquivos, o IMAP é usado para acessar e-mails em um servidor remoto, o SMTP é usado para enviar e-mails e o POP é usado para baixar e-mails de um servidor remoto (Letra E).

#VamosPraticar#

Web: HTTPS

Hypertext transfer protocol SECURE (https)
Protocolo da camada de aplicação utilizado para carregar páginas da web, enviar formulários, realizar transações online, obter recursos, entre outros, porém com uma camada adicional de segurança entre o cliente e o servidor. Possui recursos para criptografar a comunicação, protegendo a troca de dados contra interceptação e alteração. Esse protocolo requer certificados digitais para autenticar a identidade do servidor e garante que os dados transferidos sejam acessíveis apenas para o destinatário pretendido. Além disso, ele verifica

se os dados enviados não foram alterados ou corrompidos durante a transferência e confirma a identidade do site para o usuário.

O HTTPS é um protocolo que tem a mesma finalidade do HTTP. Em outras palavras, ele é responsável pela transferência, formatação e apresentação de páginas web com conteúdo multimídia (textos, áudio, imagens, entre outros) entre um servidor e um cliente. No entanto, ele realiza transferências de forma segura, oferecendo criptografia, autenticação e integridade às transferências de dados de/para um servidor web. **Trata-se de uma implementação do HTTP sobre uma camada adicional de segurança que utiliza um outro protocolo chamado SSL/TLS** [49]. Esses protocolos possuem propriedades criptográficas que permitem assegurar confidencialidade e integridade à comunicação.

Dessa forma, é possível que os dados sejam transmitidos por meio de uma conexão criptografada e que se verifique a autenticidade do servidor web por meio de certificados digitais.

#VamosPraticar#

(FGV / SEFAZ-ES – 2022) Sites cujos endereços são iniciados por "HTTPS://" garantem maior grau de segurança no acesso à Internet, quando comparados com aqueles iniciados por "HTTP://". Assinale a opção que apresenta um fator relevante para a disseminação do protocolo HTTPS.

a) Criptografia das mensagens.

b) Rapidez no acesso.

c) Suporte a diferentes navegadores.

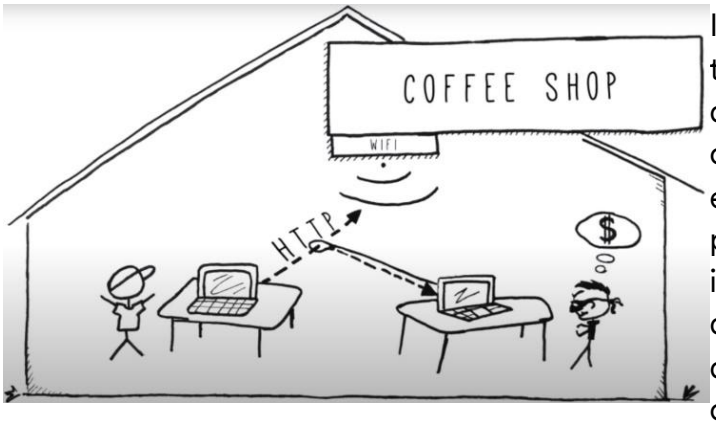
d) Suporte a idiomas estrangeiros.

e) Suporte a múltiplas plataformas de hardware.

Comentários: (a) Correto. A criptografia das mensagens é um dos fatores primordiais para a disseminação do protocolo HTTPS. Este protocolo adiciona uma camada de segurança (SSL/TLS) ao HTTP, garantindo a confidencialidade e integridade dos dados durante a transmissão; (b) Errado. Apesar de desejável, a rapidez no acesso não é um fator diretamente

relacionado com a disseminação do HTTPS. A segurança adicional oferecida pelo HTTPS pode, em algumas situações, até implicar em uma ligeira redução na velocidade de carregamento das páginas; (c) Errado. O suporte a diferentes navegadores é uma característica importante, mas não é um fator específico para a disseminação do HTTPS, visto que tanto o HTTP quanto o HTTPS são suportados pela maioria dos navegadores modernos; (d) Errado. O suporte a idiomas estrangeiros é uma característica relacionada ao conteúdo dos sites e não tem relação direta com o protocolo de transmissão (HTTP ou HTTPS); (e) Errado. O suporte a múltiplas plataformas de hardware está mais relacionado ao design e desenvolvimento de sites e aplicações web, não sendo um fator decisivo para a escolha entre HTTP e HTTPS (Letra A).

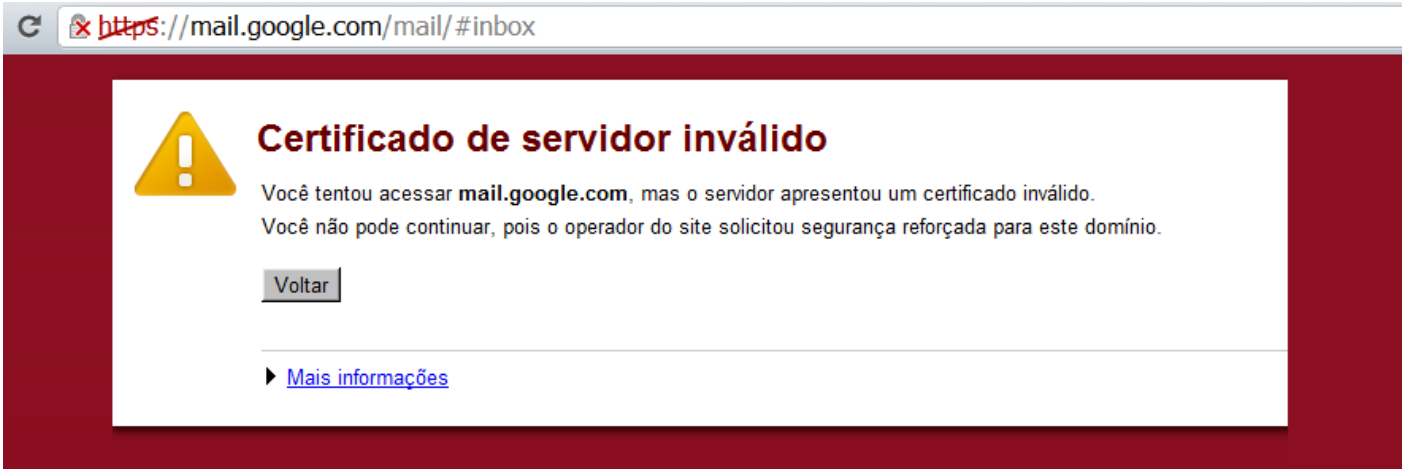
#VamosPraticar#



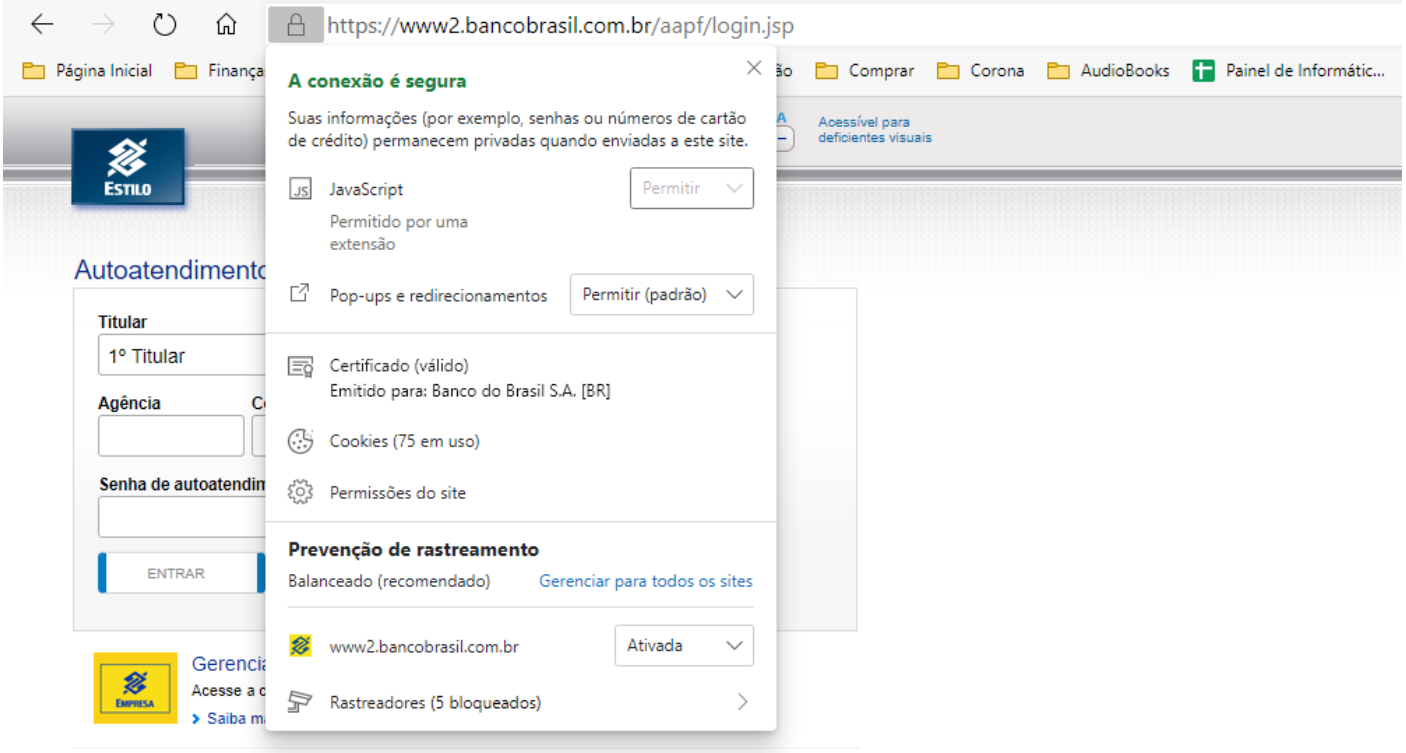
Imagine que você está em um Coffee Shop, tomando seu cafezinho com seu notebook e decide comprar um presente para sua mãe online em um site que utiliza apenas o HTTP e, não, HTTPS. Uma pessoa na mesa ao lado pode utilizar métodos maliciosos para interceptar sua transação e descobrir os dados do seu cartão de crédito, uma vez que seus dados estão trafegando em claro (sem criptografia).**Por meio da utilização do HTTPS, a mensagem será criptografada e permanecerá ilegível mesmo que seja interceptada por usuários não autorizados.** Agora imaginemos outro cenário...

Você procura no Google um site bacana para comprar o presente. Entre os links encontrados, você lê rápido e não percebe que, na verdade, acessou a amason.com [50] em vez da amazon.com [51]. Esse primeiro site é igualzinho ao original, mas foi feito por um hacker para você pensar que se trata do mesmo site e roubar os dados do seu cartão de crédito. *E agora, professor?*

Nesse momento, seu navegador solicitará ao site um documento chamado Certificado Digital. Esse documento é simplesmente uma maneira de validar se um site é realmente quem diz ser, isto é, de uma empresa legítima. **Um site legítimo envia as informações da empresa a uma autoridade certificadora registrada para criar um certificado digital e permitir que usuários acessem sua página de forma segura.**



Após recebê-lo, o navegador consulta diversas autoridades públicas e privadas para verificar se esse certificado é válido – é como se alguém enviasse uma assinatura e você fosse a vários cartórios para conferir se aquela assinatura era legítima ou não. *Sabe quando você tenta acessar uma página e o navegador avisa que o certificado é inválido?* **Pois é, isso significa geralmente que o certificado não foi encontrado, expirou ou foi revogado.** Logo, tomem cuidado com esse tipo de mensagem!



Exemplo: se você entrar em um site de um Internet Banking, você visualizará o endereço começando com **https://** e um pequeno cadeado do lado esquerdo da barra de endereço indicando que a conexão a essa página é segura. *Por que?* Porque veja que é informado que o certificado já foi recebido, já foi verificado e foi considerado válido. Galera, é claro que isso não é uma garantia absoluta, é apenas uma forma de garantir que a informação trafegada estará segura.

#VamosPraticar#

(CESPE / Telebrás – 2022) https://www.telebras.com.br/ [52] é uma URL em que HTTPS indica o protocolo de comunicação, com uma camada de proteção na transmissão de dados, entre o computador de um usuário e o servidor, que permite a obtenção de recursos textuais do sítio da TELEBRAS.

Comentários: essa URL utiliza o protocolo HTTPS. Este protocolo é uma versão segura do HTTP e inclui uma camada adicional de segurança (SSL/TLS) para proteger os dados durante a transmissão entre o computador do usuário e o servidor. Isso garante a integridade e a confidencialidade dos dados enviados e recebidos, prevenindo a interceptação ou alteração por terceiros. O HTTPS é especialmente importante para a transferência de informações sensíveis, como dados pessoais e financeiros. A referência a "recursos textuais do sítio da TELEBRAS" se alinha com a função do protocolo de transferir diversos tipos de dados e recursos da web, como páginas HTML, imagens e arquivos (Correto).

(IBFC / MGS – 2019) O protocolo mais popular de transferência de dados na internet, HTTP (do inglês Hypertext Transfer Protocol) teve desenvolvida, ao longo da última década, uma variação com maior segurança, o chamado HTTPS. O HTTPS utiliza uma combinação dos protocolos de comunicação criptografados TLS (Transport Layer Security) ou SSL (Secure Sockets Layers, em inglês). Sobre esse assunto, analise as afrmativas abaixo, dê valores Verdadeiro (V) ou Falso (F).

( ) Os sites que são acessados a partir de um protocolo de transferência de hipertexto seguro, aparecem com o código “https://” antes da URL.

( ) No HTTPS há uma conexão de dados segura entre o computador do usuário e o servidor, usando criptografa, que procura dificultar a interceptação das informações durante a transmissão dos dados entre o computador do usuário e os servidores dos sites.

( ) Hipertexto é implementado na linguagem html que é uma linguagem de programação de sites e que possibilita programar técnicas de criptografa.

( ) No Google Chrome, desde a versão de 2018, sites HTTP sem a camada de segurança aparecem marcados em vermelho com a advertência “Inseguro”.

Assinale a alternativa que apresenta, de cima para baixo, a sequência correta.

a) V, F, F, V

b) F, F, V, F

c) F, V, V, F

d) V, V, F, V

Comentários: (I) Correto. Sites que utilizam HTTPS mostram "https://" antes da URL, indicando que a conexão é segura; (II) Correto. O HTTPS cria uma conexão segura entre o navegador do usuário e o servidor, utilizando criptografia para proteger os dados transmitidos; (III) Errado. HTML (Hypertext Markup Language) é uma linguagem de marcação usada para criar páginas na Web. Ela não é uma linguagem de programação e não possui funcionalidades inerentes para programar criptografia; (IV) Correto. Desde 2018, o Google Chrome começou a marcar sites HTTP como "Inseguros", incentivando a adoção do HTTPS para uma navegação mais segura (Letra D).

#VamosPraticar#

Protocolo FTP

INCIDÊNCIA EM PROVA: ALTÍSSIMA
FILE TRANSFER PROTOCOL (FTP)
Protocolo da camada de aplicação baseado no modelo cliente/servidor utilizado para a transferência de arquivos entre sistemas. Ele pode transferir uma variedade de tipos de dados (incluindo arquivos binários e de texto), além de permitir upload e download de arquivos, além de suporte a comandos para manipulação de diretórios. Ademais, requer autenticação (nome de usuário e senha) para acesso, embora possa ter acesso anônimo. O FTP é amplamente utilizado para distribuição de arquivos, backup e transferência de dados entre sistemas.

O FTP (File Transfer Protocol) **é o protocolo responsável pela realização de transferências de arquivos entre um Cliente FTP e um Servidor FTP**. Definições que já encontrei em prova:

> *- FTP é o protocolo de transferência de arquivos entre computadores;*
>
> *- FTP é o protocolo para transferência de arquivos entre dois computadores conectados à Internet;*
>
> *- FTP é o protocolo responsável pela transferência de arquivos remotos;*

> *- FTP é o protocolo que permite a cópia de arquivos entre dois computadores;*
>
> *- FTP é o protocolo responsável pelo download/upload de arquivos;*
>
> *- FTP é o protocolo que permite fazer upload de arquivos para um servidor remoto.*

Esse protocolo difere de outros por estabelecer duas conexões entre cliente e servidor: **uma para a transferência dos dados em si (Porta TCP 20) e a outra para a troca de informações de controle (Porta TCP 21).** Essa divisão ocorre para tornar o protocolo mais eficiente, visto que as informações de controle utilizam uma conexão mais simples, enquanto a transferência de dados possui uma conexão mais complexa, permitindo o envio de múltiplos arquivos, etc.

É comum que empresas disponibilizem um Servidor FTP e as máquinas dos usuários possuam Clientes FTP. **Dessa forma, diversos clientes podem fazer o upload de arquivos para o servidor, que funcionará como um repositório central de arquivos.** Da mesma forma, clientes poderão fazer o download dos arquivos do repositório. O FTP permite fazer download, upload, renomeação, exclusão de arquivos de forma geralmente autenticada. Existem diferentes modos de transmissão:

MODO DE TRANSMISSÃO	DESCRIÇÃO
FLUXO CONTÍNUO (STREAM)	O arquivo é enviado, por um fluxo contínuo de bytes, ao TCP. Quando chega nesse protocolo, ele separa os dados recebidos em porções com um tamanho apropriado para o transporte – trata-se do modo-padrão.
BLOCADO	Os dados são entregues do FTP para o TCP em blocos. Nesse caso, cada bloco é precedido por um cabeçalho de três bytes. O primeiro byte é chamado de descritor de blocos; os dois seguintes definem o tamanho do bloco em bytes.
COMPRIMIDO	No caso de arquivos muito grandes, os dados podem ser comprimidos, antes de serem enviados, usando um algoritmo.

Galera, por que nós utilizamos a internet? Basicamente para nos comunicar! E para haver comunicação, são necessárias duas partes: um emissor e um receptor. Quando você acessa um portal da web, quando você faz o download de um arquivo, quando você joga um jogo na internet, quando você acessa uma rede social ou quando você vê um vídeo no Youtube **sempre haverá transferência (envio ou recebimento) de informações**.

Por falar nisso, há dois termos que eu tenho certeza que vocês estão bastante familiarizados porque já fazem parte do nosso vocabulário em português: Download e Upload! Nós já sabemos que a Internet funciona por meio de uma arquitetura ou modelo chamado Cliente/Servidor! *O que é isso, professor?* **Grosso modo, isso significa que ela é baseada em um conjunto de computadores que exercem a função de clientes ou servidores**. Relembrando...

Os computadores servidores são aqueles que fornecem um serviço e os computadores clientes são aqueles que consomem um serviço. *Sabe aquele domingo à noite em que quer ver um filme maneiro?* Você liga sua televisão, acessa a página web da Netflix, escolhe um filme e começa a assisti-lo! Nesse momento, sua televisão funciona como um cliente que está consumindo um serviço. *Esse serviço é disponibilizado por quem?* Pela Netflix!

A Netflix possui um bocado de computadores servidores que hospedam ou armazenam os filmes, então a sua televisão está consumindo um serviço de um servidor da Netflix. E quase tudo na internet é assim: você acessa o servidor do Estratégia para ver uma videoaula; você acessa o servidor do Spotify para ouvir uma música; você acessa o servidor do Google para acessar sua página e fazer alguma busca; e assim por diante. Dito isso, vamos ver o que é download e upload...

Ambos os termos são utilizados para referenciar a transmissão de dados de um dispositivo para outro através de um canal de comunicação previamente estabelecido. **O termo download está relacionado com a obtenção de conteúdo da Internet, em que um servidor hospeda dados que são acessados pelos clientes através de aplicativos específicos que se comunicam com o servidor por meio de protocolos preestabelecidos** (Ex: HTTP, FTP, etc).

De forma análoga, o termo upload faz referência a operação inversa à do download, isto é, refere-se ao envio de conteúdo à internet**. Do ponto de vista da participação do dispositivo que iniciou a transmissão de dados, a obtenção de dados de um dispositivo é chamada de download e a disponibilização de dados para um dispositivo é chamada de upload.** *Tudo certo?* Então, vamos prosseguir...

Eu já recebi essa dúvida no fórum dezenas de vezes, portanto vamos tentar deixar bastante claro para não haver margem para questionamentos! **O objetivo principal do FTP é transferir arquivos, no entanto nem toda transferência de arquivos ocorrerá por FTP.** *É possível transferir arquivos por e-mail?* Sim, nesse caso estaremos utilizando SMTP/MIME. *É possível transferir arquivos por uma página web?* Sim, nesse caso estaremos utilizando HTTP/HTTPS.

Quando você faz o download de uma aula ou vídeo em nosso site, você está utilizando o HTTP para transferência de arquivos do servidor web para a sua máquina local. **Em suma: HTTP é utilizado para transferência de hipertexto, mas pode ser utilizado alternativamente para transferência de arquivos; SMTP é utilizando para transferência de e-mails, mas pode ser utilizado alternativamente para transferência de arquivos; e existem dezenas de outros exemplos.**

Diversos outros protocolos possuem seus objetivos principais, mas alternativamente também permitem enviar arquivos – já o objetivo principal do FTP é a transferência de arquivos. A grande verdade é que o FTP tem sido cada vez menos utilizado – principalmente após a popularização do armazenamento em nuvem (Cloud Storage). Eu arrisco dizer que a maioria de vocês nunca usou esse protocolo em toda vida, apesar de fazer transferência de arquivos há anos na internet.

Há algum tempo, esse protocolo permanecia sendo utilizado para transferência de arquivos muito grandes. Hoje em dia, eu faço o upload do arquivo grande para nuvem e envio o link para quem eu quiser – sem precisar configurar um Cliente/Servidor FTP. Apesar de estar em desuso, ele continua sem bastante cobrado em prova. **Por essa razão, muito cuidado para não achar que toda transferência de arquivos ocorre por meio do FTP.**

#VamosPraticar#

(SEFAZ/ES – 2011)

O FTP, protocolo de transferência de arquivos, é utilizado toda vez que o usuário baixa um arquivo armazenado em um sítio web ou, então, quando anexa arquivo a mensagem de correio eletrônico.

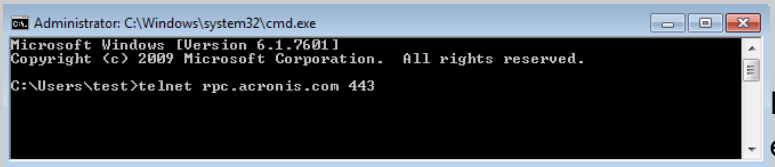
Comentários: opa... um usuário utiliza HTTP/HTTPS para transferência de arquivos de um sítio web e, não, FTP (Errado).

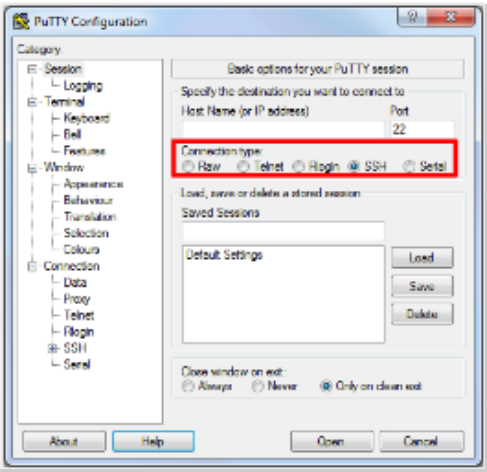
#VamosPraticar#

Protocolos Diversos

INCIDÊNCIA EM PROVA:BAIXÍSSIMA

Agora veremos alguns protocolos que caem muito muito muito raramente em prova, portanto veremos bem rápido. Acompanhem a tabela seguinte...

PROTOCOLOS	DESCRIÇÃO
TELNET	Trata-se de um protocolo cliente/servidor utilizado para permitir a comunicação remota entre computadores em uma rede de computadores. Ele proporciona uma facilidade de comunicação baseada em texto interativo bidirecional utilizando um terminal virtual, isto é, ele não permite o controle remoto da interface gráfica – permite apenas executar comandos em um terminal de outro computador. Vejam como ele é...  Ele permite, por exemplo, acessar um computador remoto e executar um comando para desligá-lo. Nesse contexto, a máquina que oferece o acesso remoto é o servidor e o equipamento que acessa é o cliente. O TELNET não garante uma comunicação segura, até dados e senhas são compartilhados em texto livre durante a conexão. Esse protocolo está obsoleto há anos, por conta de novos protocolos mais eficientes e por possuir diversos problemas de segurança.
SSH	Trata-se de um protocolo cliente/servidor de acesso remoto que utiliza autenticação de chave pública baseada no servidor para estabelecer a identidade do usuário com segurança e oferecer. A principal diferença para o protocolo anterior é que ele utiliza criptografia, o que garante confidencialidade e integridade de dados sobre uma rede insegura (como a Internet) e que os dados transmitidos na rede estejam seguros contra interceptações não autorizadas.

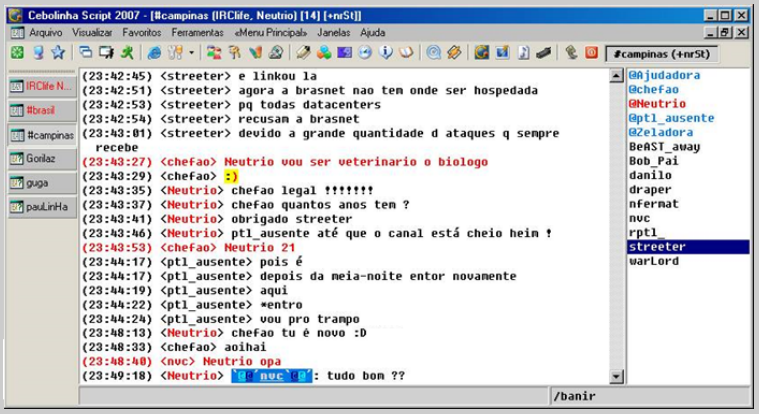


Se vocês já trabalharam em alguma empresa grande, já devem ter ligado para um técnico de informática detalhando algum problema que foi resolvido remotamente. O técnico de suporte acessa o seu computador, realizando todas as manutenções ou correções requisitadas. Existem softwares que implementam diversos protocolos de acesso remoto (inclusive sobre sistemas operacionais diferentes) – uma das mais conhecidas é o PuTTY.

IRC

Trata-se de um protocolo cliente/servidor utilizado basicamente para bate-papo e troca de arquivos, permitindo uma conversa em grupo ou privada (IRC – *Internet Relay Chat*). Quem é mais antigo sabe que antigamente a única maneira de falar com outra pessoa era por meio de um telefone. Quando eu, com uns oito anos de idade, vi um Cliente IRC pela primeira vez e descobri que era possível falar com outra pessoa pelo computador, eu achei genial!

O Cliente IRC mais comum era o mIRC! Era lento e feio, mas para quem não tinha nada, era uma das melhores coisas do mundo. Crianças, eu vos apresento a comunicação via computador dos anos 90:



SNMP	Trata-se de um protocolo para monitoramento e gerenciamento de dispositivos em uma rede de computadores (SNMP – *Simple Network Management Protocol*). Para tal, esse protocolo coleta um conjunto de métricas de diversos dispositivos, tais como roteadores, computadores, servidores, entre outros. Ele opera sobre o Protocolo UDP na Porta 161 e está atualmente em sua terceira versão – SNMPv3.
RTP	Trata-se de um protocolo para transmissão de áudio e vídeo em tempo real sobre Redes IP (RTP – *Real-time Transport Protocol*). Ele é comumente utilizado em aplicações VoIP e opera sobre o Protocolo UDP. Existe uma polêmica sobre a camada em que opera esse protocolo – alguns afirmam que se trata da camada de transporte e outros afirmam que se trata da camada de aplicação. Lembrem-se que nem sempre é possível alocar perfeitamente um protocolo a uma camada.
NNTP	Trata-se de um protocolo da camada de aplicação utilizado para grupos de discussão, permitindo especificar, buscar, recuperar e postar artigos usando um sistema de transmissão confiável. Ele também era útil para leitura de notícias em tempos remotos. Esse protocolo encontra-se obsoleto e está em desuso há muito anos, mas vez ou outra cai em prova.

TELNET	SSH
NÃO! NÃO TEM CRIPTOGRAFIA	**SIM! TEM CRiPTOGRAFIA**

#VamosPraticar#

(FUNDATEC / PROCERGS – 2023) A função principal do Telnet é:

a) Acessar correio eletrônico (e-mail).

b) Acessar newsgroups.

c) Realizar logon remoto.

d) Realizar transferência de arquivos.

e) Navegar na internet.

Comentários: (a) Errado, essa seria a função principal do POP3/IMAP; (b) Errado, essa seria a função principal do NNTP; (c) Correto; (d) Errado, essa seria a função principal do FTP; (e) Errado, essa seria a função principal do HTTP/HTTPS (Letra C).

(CESPE / PG-DF – 2021) O SNMP (Simple Network Management Protocol) tem como função fazer a conexão segura (criptografada) a determinado computador da rede e, dependendo do nível de acesso e privilégios, controlar esse computador remotamente.

Comentários: SNMP tem a função de coletar informações e monitorar a rede, ele não é focado em controle remoto ou criptografia. Na verdade, a questão trata do SSH (Errado).

#VamosPraticar#

Redes de Computadores - Parte 2 - Serviço VoIP - Teoria

Serviço VoIP

INCIDÊNCIA EM PROVA: MÉDIA

Voip
VoIP (Voice over Internet Protocol) é uma tecnologia que permite a transmissão de voz e comunicações multimídia (como chamadas telefônicas, videotelefonia e sessões de conferência) através da Internet ou de outras redes baseadas em protocolos IP. Essencialmente, o VoIP transforma sinais de voz em dados digitais que podem ser enviados pela internet, como qualquer outro tipo de dado.

Nas últimas décadas, popularizou-se a tecnologia de VoIP – também chamada de Voz sobre IP ou Telefonia IP [53]. Essa tecnologia permitiu sair de uma transmissão analógica para transmissão digital. A voz que era convertida em sinais elétricos, agora era convertida em sinais digitais (0's e 1's) e viajava sobre a infraestrutura da Internet. *Como é?* Pois é, nada de utilizar a infraestrutura de redes telefônicas convencionais e sua antiga comutação por circuitos.

#VamosPraticar#

(CESPE / FUB – 2022) VoIP é uma tecnologia que utiliza a Internet para realizar chamadas telefônicas.

Comentários: ele realmente é uma tecnologia que permite realizar chamadas telefônicas através da Internet. Ela converte sinais de voz em pacotes de dados digitais que podem ser transmitidos por redes baseadas em IP, como a Internet. Isso permite que os usuários façam e recebam chamadas usando a Internet, em vez de usar as redes telefônicas tradicionais (Correto).

#VamosPraticar#

Vamos detalhar isso melhor: as redes telefônicas convencionais são chamadas de **PSTN (Public Switched Telephone Network).** Trata-se de redes que utilizam comutação por circuitos, em que é estabelecido um caminho dedicado e contínuo entre dois pontos para a duração da chamada. Este método é menos eficiente em termos de largura de banda do que a comutação por pacotes, sendo progressivamente substituído por tecnologias baseadas em IP, como o VoIP.
Já o VoIP utiliza a infraestrutura da Internet e a comutação por pacotes – também conhecido como **Roteamento de Conversação de Voz!** A comutação por pacotes é mais eficiente para redes modernas, pois permite o uso mais flexível e eficiente da largura de banda disponível, além de suportar uma variedade de outros serviços. A voz é convertida em pacotes de dados e transmitida pela internet ou outras redes baseadas no Internet Protocol (IP).

#VamosPraticar#

(IGEDUC / Prefeitura de Surubim-PE – 2023) A tecnologia VoIP (Voz sobre IP) é uma forma de comunicação telefônica que utiliza redes de computadores e a Internet para transmitir chamadas de voz, tornando-as mais econômicas do que as chamadas telefônicas tradicionais.

Comentários: de fato, é uma forma de comunicação telefônica que utiliza redes de computadores, incluindo a Internet, para transmitir chamadas de voz. Essa tecnologia converte sinais de voz em pacotes de dados digitais, que são então transmitidos através de redes IP.

Uma das vantagens significativas do VoIP é a redução de custos, especialmente notável em chamadas de longa distância e internacionais, comparativamente às chamadas telefônicas tradicionais que utilizam redes de telefonia convencionais (Correto).

(CESPE / Polícia Federal – 2013) As redes de telefonia modernas estão migrando em grande parte para a tecnologia VoIP, em que é empregada comutação por circuitos, diferentemente das redes PSTN (Public Switched Telephone Network) tradicionais, que empregam comutação por pacotes.

Comentários: na verdade, VoIP emprega a comutação por pacotes e PSTN emprega a comutação por circuitos (Errado).

#VamosPraticar#

Galera, quando falamos sobre infraestrutura da Internet, estamos nos referindo aos dispositivos, aos cabeamentos, aos algoritmos, às técnicas, às ferramentas, aos paradigmas e, por fim, à pilha de protocolos que rege toda a comunicação entre dispositivos da Internet – **também chamada de Arquitetura TCP/IP**. Agora vocês devem estar se perguntando como exatamente tudo isso funciona. Então vejam só...

Nós já sabemos que a telefonia digital transforma a voz em sinais digitais. **Esses sinais digitais são encapsulados pelo Protocolo IP em milhares de pequenos pacotinhos contendo entre 10 e 30 milissegundos de áudio.** Nós sabemos também que os principais protocolos utilizados para transporte na Internet são o TCP e o UDP. Agora eu tenho uma pergunta: vocês acham que o VoIP utiliza qual desses protocolos?

Lembrem-se que o TCP é aquele protocolo que realiza uma conexão prévia antes de transferir os dados e que realiza um controle para garantir que as informações sejam entregues em perfeito estado, logo ele é um protocolo confiável e orientado à conexão. **Já o UDP é aquele protocolo que não realiza conexão prévia antes de transferir os dados e nem garante a entrega ao destinatário, logo ele é um protocolo não confiável e não orientado à conexão.**

Agora vamos imaginar um cenário em que eu desejo te enviar um áudio que eu gravei tocando sanfona. Se eu te enviar esse áudio por meio do Protocolo UDP e houver uma perda de pacotes no meio do caminho, você receberá o áudio faltando partes. Imagine só... vai perder a introdução da música, por exemplo, que eu toquei com todo carinho. **Nesse caso, é importante que você receba os dados, logo é mais interessante utilizar o Protocolo TCP em vez do Protocolo UDP.**

Agora vamos imaginar outro cenário em que você deseja me ligar para avisar que passou no concurso público dos seus sonhos. Eu atendo sua ligação, mas volta e meia há um corte ou uma pequena interrupção. *Ora, faz sentido eu receber depois essas partes que foram perdidas?* Não, perdeu, já era! **Nesse caso, é mais interessante utilizar o Protocolo UDP em vez do Protocolo TCP.***E em qual contexto se encaixa o uso do VoIP?* No segundo, porque ele utiliza o UDP!

Professor Diego... eu posso afirmar que ele utiliza um serviço com conexão não confiável e não orientado à conexão? Não! *Como não?* Aqui há um detalhe: VoIP utiliza outro protocolo (SIP ou H.323) junto com o UDP para garantir o estabelecimento de uma conexão com o destinatário. Logo, podemos afirmar que uma aplicação VoIP é orientada à conexão e não-confiável. **O foco aqui é na simplicidade e na agilidade da comunicação.**

VANTAGENS DO VOIP
- Permite fazer e receber ligações telefônicas tanto em uma rede local (LAN/Interna) quanto em uma rede pública (WAN/Externa).
- Permite fazer e receber ligações para telefones fixos ou telefones celulares da telefonia convencional ou da telefonia digital por meio da utilização de um conjunto de dispositivos (adaptadores, gateways, etc).
- Permite compartilhar o canal de comunicação de dados com outros serviços, podendo transmitir – além da voz – vídeos, imagens, entre outros.
- Permite uma instalação extremamente escalável, podendo expandir com facilidade sem a necessidade de novas linhas dedicadas e aproveitando a infraestrutura de Redes IP – [54].

No entanto, a maior vantagem é a redução de custos de ligação. Na telefonia convencional, a cobrança se dá por tempo e pelo tipo de ligação, com valores diferentes, dependendo da distância (ligações locais, interurbanas e internacionais), operadora (mesma operadora ou concorrente), horários (chamadas diurnas ou noturnas) e dos dias (dia de semana ou final de semana). Já por meio do VoIP, é possível reduzir valores de ligações em até 70%.

desVANTAGENS DO VOIP
- Pode oscilar e perder a qualidade da ligação caso não esteja disponível uma conexão eficiente com a Internet.
- Menos confiável que a telefonia convencional em relação a quedas de energia.
- Podem ocorrer problemas de latência, atraso, interrupção e cortes na comunicação, além de perdas de dados.
- Apresenta menor disponibilidade do canal de comunicação, uma vez que não possui um canal dedicado.

Convergência de Redes

Nós vimos que uma das vantagens dessa tecnologia era a capacidade de transmitir outros dados além da voz. Aqui é importante destacar um conceito fundamental chamado Convergência de Rede. *O que é isso, Diego?* **Trata-se de uma tendência tecnológica atual que visa unificar a infraestrutura de duas ou mais redes distintas em uma única rede de computadores capaz de prover os serviços prestados antes pelas outras redes.**

Antigamente, havia a ideia de que as redes de comunicação deveriam ser segmentadas de acordo com o tipo de serviço. Logo, deveríamos ter uma rede de comunicação para envio de voz, outra rede para envio de imagens, outra rede para envio de vídeos, outra rede para envio de documentos em geral, e assim por diante. **A convergência de redes nos trouxe a ideia de utilizar uma única rede de comunicação compartilhada com o objetivo de oferecer diferentes tipos de serviços.**

Uma rede convergente permite o tráfego de voz, imagem e dados em uma mesma rede digital, atuando de forma integrada, o que possibilita uma melhor gestão da tecnologia, a um custo mais reduzido. O maior exemplo de convergência de redes é o VoIP! Empresas podem integrar melhor a equipe com desvio de chamadas, conferências, trabalho remoto, utilização de URA, fila de chamadas em espera com música, caixa postal, identificação da transferência, entre outros.

Videoconferências

Por fim, vamos falar sobre conferências! Galera, o período de Pandemia do COVID-19 fez com que a utilização de recursos e tecnologias de conferências virtuais virassem uma tendência mundial. *Quem não viu as imagens acima circulando por aí?* Na primeira, o Ministro do STJ que apareceu com um tubarão no fundo da tela inserido por seu neto e que ele não conseguiu tirar. Na segunda, um padre italiano foi celebrar uma missa pelo Instagram e – sem querer – inseriu filtros engraçados.

Pois é, esse assunto deve se tornar uma constante em concursos futuros na medida em que órgãos públicos já vinham há anos implantando modalidades de teletrabalho para seus servidores. **A ideia é promover reuniões entre equipes, parceiros e clientes ou ações específicas de comunicação interna.** Essa solução reduz custos e agiliza esses processos – as equipes não precisam se deslocar até o local da reunião e as empresas economizam com o transporte/passagens dos colaboradores.

De modo geral, a videoconferência pode ser definida como a tecnologia que permite a interação visual e sonora entre que pessoas que estão em locais diferentes, dando a sensação – na medida do possível – de que os interlocutores se encontram em um mesmo local. **Sendo mais rigoroso, há diferenças entre webconferências e videoconferências.** *Quais, Diego?* A primeira geralmente é mais simples e utilizada em ambientes domésticos e a segunda em ambientes corporativos.

A primeira geralmente utiliza equipamentos básicos como smartphones, notebooks e webcams e a segunda geralmente utiliza equipamentos mais sofisticados como câmeras específicas para apresentação de documentos e geralmente ocorrem em salas equipadas para esse tipo de reunião. **Por fim, a primeira geralmente utiliza softwares como Hangouts, Skype, Messenger e Whatsapp; e a segunda geralmente utiliza softwares como Zoom e Teams.**

Com a pandemia, todas essas diferenças têm desaparecido, mas é interessante saber que já houve essa diferenciação. Por fim, é importante mencionar que – quando duas câmeras estão conectadas – esse sistema é chamado de ponto-a-ponto; e quando três ou mais câmeras estão conectadas, o sistema é chamado multiponto. **Nesse último, geralmente há um equipamento ou software chamado MCU (Unidade de Controle Multiponto) utilizado para conectar as câmeras.**

Também há dois modos de funcionamento da videoconferência: no Modo VAS (Switch Ativado por Voz), a janela de vídeo que fica em destaque é a da pessoa que estiver falando no momento; já no Modo Presença Contínua, as janelas de todas as câmeras conectadas são exibidas simultaneamente. É isso, galera... tópico tranquilo e pouco cobrado em prova! Espero que tenham entendido e, qualquer coisa, perguntem no fórum!

Redes de Computadores - Parte 2 - Resumo

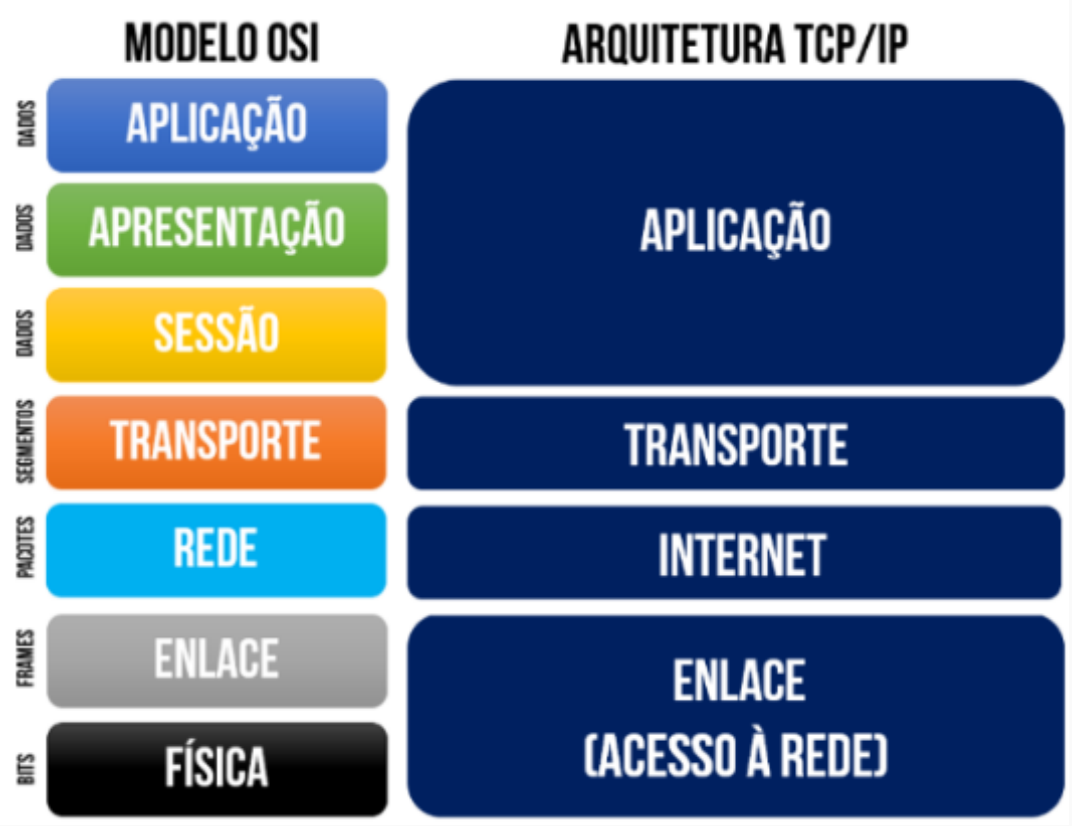
Resumo

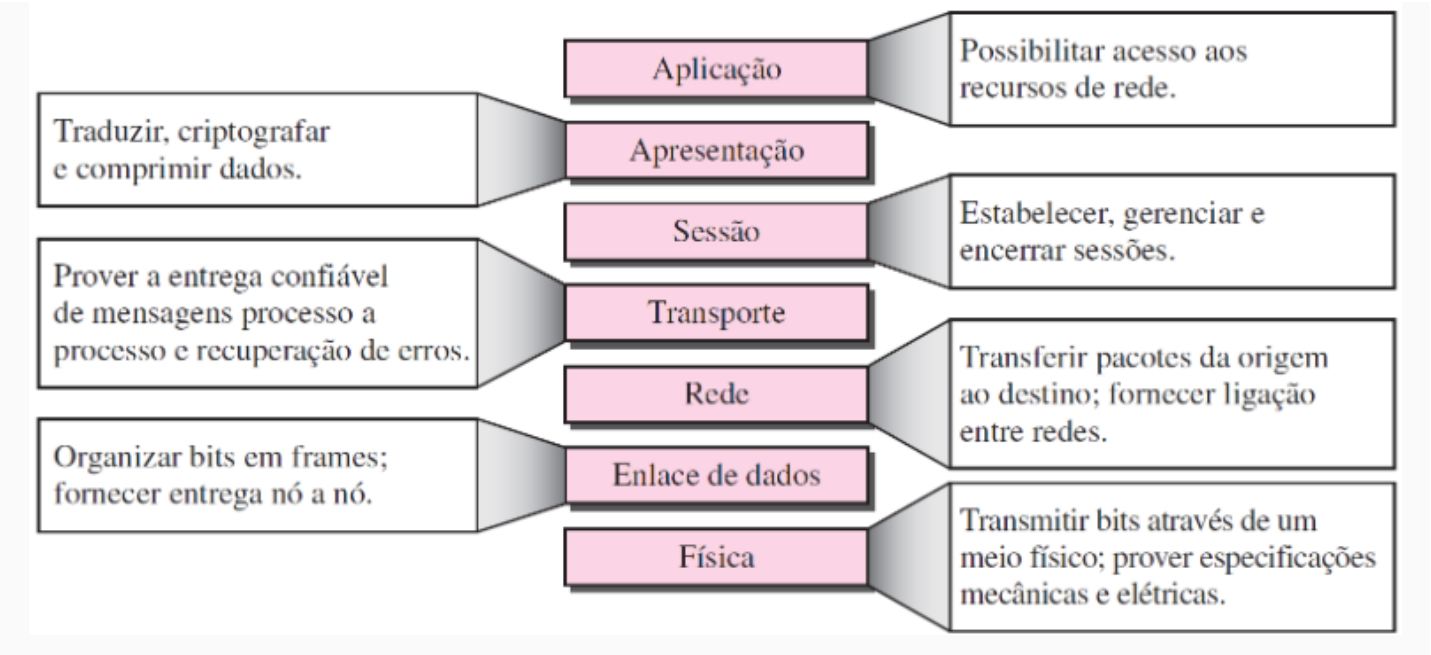
MODELO OSI

Abstração teórica, uma referência conceitual para entender como se dá o fluxo de dados entre computadores em uma rede. Ele não especifica ou prescreve protocolos para cada camada, mas é possível identificar quais protocolos correspondem à função de cada camada – por isso, vocês verão exemplos de protocolos abaixo.

ARQUITETURA TCP/ip

Trata-se de um conjunto de camadas e protocolos para conectar várias redes diferentes de maneira uniforme. Pessoal, como nós vimos no início da aula, esse é o conjunto de protocolos padrão da internet – se você quiser ter acesso à internet, terá que utilizar os protocolos prescritos pela Arquitetura TCP/IP.

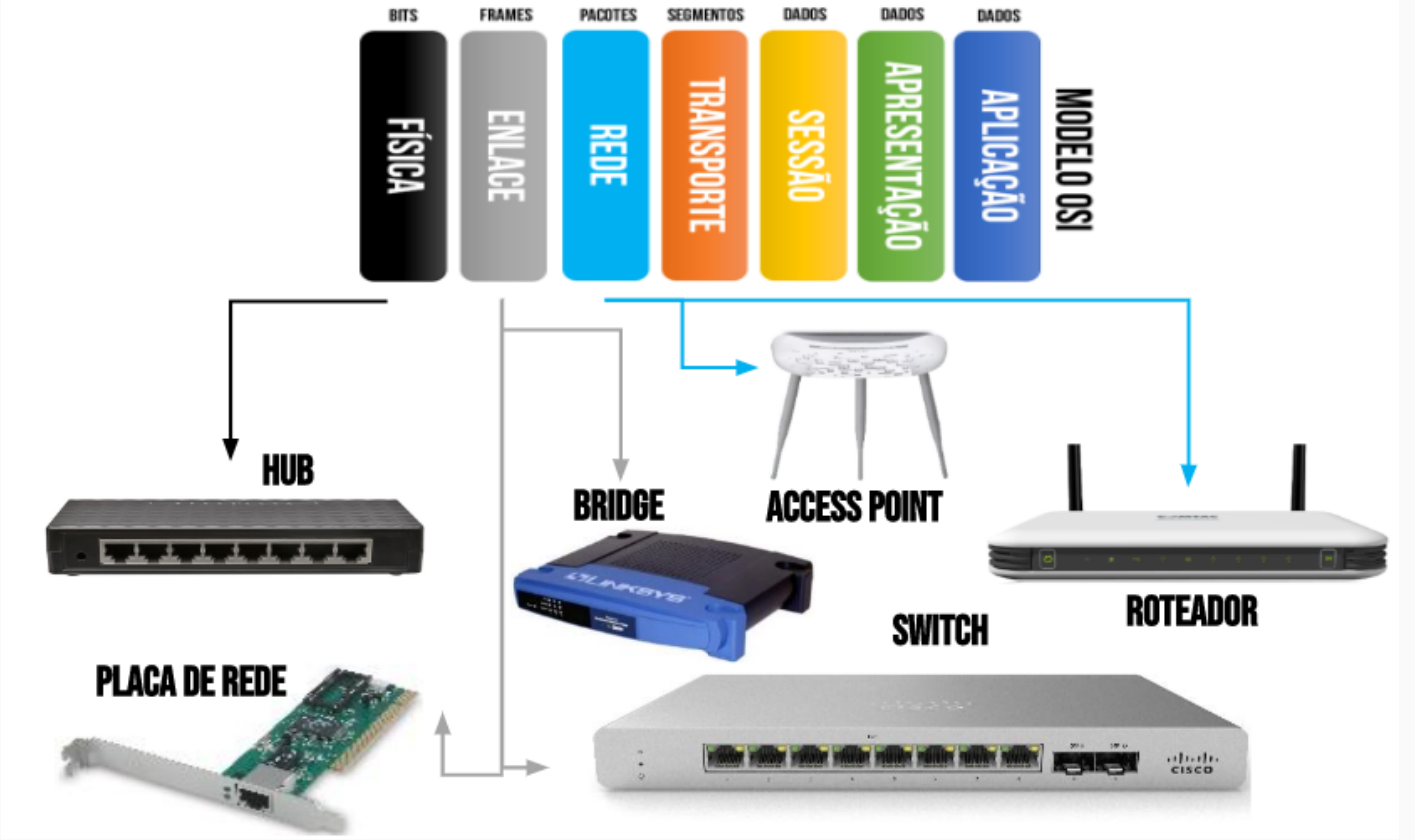




NUMERAÇÃO	CAMADA	Descrição	protocolos
7	APLICAÇÃO	Camada responsável por habilitar o usuário, seja ele humano ou software, a estabelecer a comunicação entre aplicações e a acessar a rede.	HTTP, SMTP, FTP, SSH, TELNET, IRC, SNMP, POP3, IMAP, DNS.
6	APRESENTAÇÃO	Camada responsável por definir o formato para troca de dados entre computadores, como se fosse um tradutor.	AFP, ICA, LPP, NCP, NDR, TOX, XDR, PAD.
5	SESSÃO	Camada responsável por permitir que duas ou mais aplicações em computadores diferentes possam abrir, usar e fechar uma conexão, chamada sessão.	NETBIOS.
4	TRANSPORTE	Camada responsável por organizar dados em segmentos e que eles cheguem ao destino livre de erros (sem perdas, sem duplicações e na ordem correta).	TCP, UDP, NETBEUI.
3	REDE	Camada responsável pelo endereçamento, roteamento e	IP, ICMP, ARP RARP, NAT.

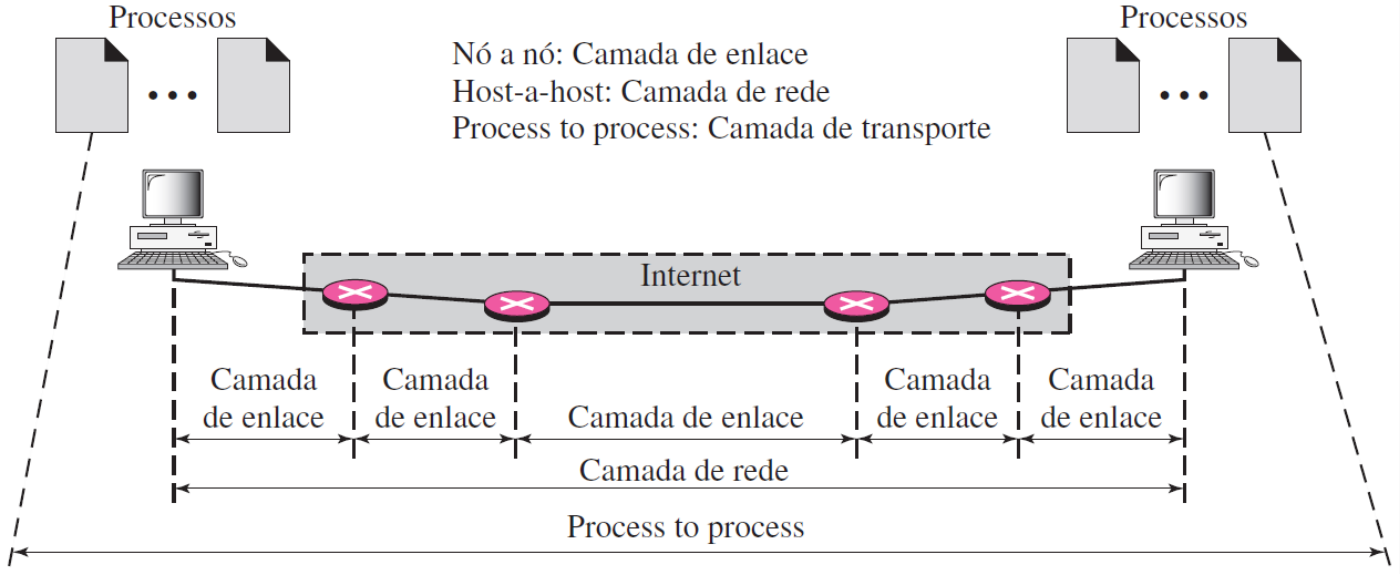
		entrega de pacotes individuais de dados desde sua origem até o seu destino, provavelmente através de várias redes.	
2	ENLACE	Camada responsável por organizar os dados em frames (ou quadros) e por estabelecer uma conexão nó-a-nó entre dois dispositivos físicos que compartilham o mesmo meio físico.	Ethernet, Token Ring, Bluetooth, Wi-Fi.
1	FÍSICA	Camada responsável por definir as especificações elétricas e físicas da conexão de dados.	USB, DSL.

MNEMÔNICO DAS CAMADAS						
F	E	R	T	S	A	A
FÍSICA	ENLACE	REDE	TRANSPORTE	SESSÃO	APRESENTAÇÃO	APLICAÇÃO
FERTlizantes				São		Assustadores
Filomeno	Enlaçou a	Rede de	Transporte do	Seu	Apolinário	Aparecido
FLAMENGO	ENSACOU NA	REDE	TRÊS	SAPECADAS NO	ATLÉTICO E	avaí



PROTOCOLO (CAMADA DE APLICAÇÃO)	PROTOCOLO (CAMADA DE TRANSPORTE)	NÚMERO DA PORTA
HTTP	TCP	80
HTTPS	TCP	443
POP3	TCP	110
SMTP	TCP	25/587
IMAP4	TCP	143
FTP	TCP	20/21
TELNET	TCP	23
SSH	TCP	22
DNS	TCP/UDP	53
DHCP	UDP	67/68

IRC	TCP	194



CAMADA	UNIDADE DE DADOS PADRAÕ	TIPO DE COMUNICAÇÃO	TIPO DE ENDEREÇO
FÍSICA	Bits	Ponto-a-Ponto	-
ENLACE	Quadros/Frames	Ponto-a-Ponto	Endereço MAC
REDE	Datagramas	Host-a-Host	Endereço IP
TRANSPORTE	Segmentos	Fim-a-Fim	Porta
SESSÃO	Mensagens	Fim-a-Fim	URL
APRESENTAÇÃO			
APLICAÇÃO			

PROTOCOLO	PORTA	DESCRIÇÃO

IP	-	Protocolo da Camada de Rede que permite a comunicação entre duas ou mais máquinas em rede para encaminhamento dos dados.
ICMP	-	Protocolo da Camada de Internet/Rede que é utilizado para comunicar a ocorrência de situações anormais na transferência de um datagrama, gerando relatórios de erros à fonte original, etc.
ARP	-	Protocolo da Camada de Rede que é responsável por manter uma tabela de conversão de endereços lógicos (IP – Camada de Rede) em endereços físicos (MAC – Camada de Enlace).
TCP	-	Protocolo da Camada de Transporte que permite o controle de transmissão confiável, entrega na sequência correta e verificação de erros dos pacotes de dados.
UDP	-	Protocolo da Camada de Transporte que fornece um serviço de entrega sem conexão e rápido, porém não confiável.
SMTP	TCP 25/587	Protocolo da Camada de Aplicação que é responsável pelo envio de e-mail através da rede. POP e IMAP recuperam e-mails de um Servidor de E-Mail – SMTP envia e-mails para um Servidor de E-Mail.
POP3	TCP 110	Protocolo da Camada de Aplicação que foi criado como uma forma simplificada para receber, baixar (fazer o download) e deletar mensagens de um Servidor de E-Mail.
IMAP	TCP 143	Protocolo da Camada de Aplicação projetado para nos livrar dos limites de envio e recebimento de e-mail de um único Cliente de E-Mail. Permite visualizar e-mails a qualquer momento de diversos dispositivos.
DHCP	UDP 67/68	Protocolo da Camada de Aplicação que configura dinamicamente endereços de rede. Em uma rede, pode ser necessário que um mesmo Endereço IP possa ser utilizado em diferentes dispositivos em momentos distintos.

DNS	**TCP/UDP** **53**	Protocolo da Camada de Aplicação responsável por atribuir endereços léxicos aos recursos da rede. Busca transformar endereços numéricos em nomes amigáveis, mais compreensíveis por humanos.
HTTP	**TCP** **80**	Protocolo da Camada de Aplicação utilizado em programas de navegação para acessar páginas web. É responsável pela transferência, formatação e apresentação de páginas web com conteúdo multimídia.
HTTPS	**TCP** **443**	Protocolo da Camada de Aplicação que tem a mesma finalidade do HTTP, mas ele realiza transferências de forma segura e criptografada, oferecendo autenticação e integridade às páginas de um Servidor Web.
FTP	**TCP** **20/21**	Protocolo da Camada de Aplicação que é responsável pela realização de transferências de arquivos entre um Cliente FTP e um Servidor FTP.
TELNET	**TCP** **23**	Protocolo da Camada de Aplicação que permite conectar dois computadores de forma que um usuário consiga efetuar login em outro computador através da rede de forma remota.
SSH	**TCP** **22**	Protocolo da Camada de Aplicação que é um protocolo de acesso remoto que utiliza autenticação de chave pública e oferece suporte à compressão de dados para a execução de aplicações com interfaces gráficas.
IRC	**TCP** **194**	Protocolo da Camada de Aplicação que é utilizado basicamente para bate-papo e troca de arquivos, permitindo uma conversa em grupo ou privada.
SNMP	**UDP** **161**	Protocolo da Camada de Aplicação para monitoramento e gerenciamento de dispositivos em uma rede de computadores (SNMP – Simple Network Management Protocol).

TCP	UDP

É comparativamente mais lento que o UDP	É comparativamente mais rápido que o TCP
Entregas confiáveis	Entregas não confiáveis (melhor esforço)
Orientado à conexão	Não orientado à conexão
Dados perdidos são retransmitidos	Dados perdidos não são retransmitidos.
Realiza controle de fluxo e congestionamento	Não realiza controle de fluxo e congestionamento
Tolera atrasos, mas não tolera perdas	Tolera perdas, mas não tolera atrasos
Envia dados em unicast	Envia dados em unicast, multicast ou broadcast
Oferece conexão ponto a ponto	Oferece conexão ponto a ponto ou ponto-multiponto
Bastante utilizada em e-mail, navegação, etc.	Bastante utilizada em VoIP, streaming, etc.

POP3	IMAP
Post Office Protocol (Version 3)	Internet Message Access Protocol
Não recomendado para acesso em múltiplos dispositivos	Recomendado para acesso em múltiplos dispositivos
Não permite criar e organizar pastas no servidor	Permite criar e organizar pastas no servidor
Não permite verificar o cabeçalho antes de baixá-lo	Permite verificar o cabeçalho antes de baixá-lo
Modificações em um dispositivo não refletidas em outros	Modificações em um dispositivo refletidas em outros
Não permite baixar parcialmente um e-mail	Permite baixar parcialmente um e-mail

Por padrão, mensagens de e-mail são lidas offline	Por padrão, mensagens de e-mail são lidas online
Não permite múltiplas caixas postais	Permite múltiplas caixas postais
Porta 110	Porta 143

SMTP	POP3	IMAP
ENVIAR	**COPIAR**	**ACESSAR**

URL – Sintaxe abstrata
PROTOCOLO://IP-OU-DOMÍNIO:PORTA/CAMINHO/RECURSO

COMPONENTES	DESCRIÇÃO
PROTOCOLO	Também chamado de esquema, trata-se do protocolo utilizado para acessar um recurso.
IP	Número de IP do Servidor que hospeda um recurso (Host).
DOMÍNIO	Nome do Domínio do Servidor que hospeda um recurso (Host).
PORTA	Ponto lógico que permite criar uma conexão em um processo.
CAMINHO	Estrutura de diretórios dentro do servidor que armazena um recurso.
RECURSO	Componente físico ou lógico disponível em um sistema computacional.

VOIP (VOICE OVER IP)
Serviço de roteamento de conversação humana por meio de uma rede de computadores.

VANTAGENS DO VOIP
- Permite fazer e receber ligações telefônicas tanto em uma rede local (LAN/Interna) quanto em uma rede pública (WAN/Externa).
- Permite fazer e receber ligações para telefones fixos ou telefones celulares da telefonia convencional ou da telefonia digital por meio da utilização de um conjunto de dispositivos (adaptadores, gateways, etc).
- Permite compartilhar o canal de comunicação de dados com outros serviços, podendo transmitir – além da voz – vídeos, imagens, entre outros.
- Permite uma instalação extremamente escalável, podendo expandir com facilidade sem a necessidade de novas linhas dedicadas e aproveitando a infraestrutura de Redes IP.

DESVANTAGENS DO VOIP
- Pode oscilar e perder a qualidade da ligação caso não esteja disponível uma conexão eficiente com a Internet.
- Menos confiável que a telefonia convencional em relação a quedas de energia.
- Podem ocorrer problemas de latência, atraso, interrupção e cortes na comunicação, além de perdas de dados.
- Apresenta menor disponibilidade do canal de comunicação, uma vez que não possui um canal dedicado.

S	M	T	P
SUA	MENSAGEM	TÁ	PARTINDO

D	N	S
DÁ	NOME AO	SITE

TELNET	SSH
NÃO! NÃO TEM CRIPTOGRAFIA	SIM! TEM CRiPTOGRAFIA

PARA MAIS DICAS: www.instagram.com/professordiegocarvalho [55]

Mapa Mental - Redes de Computadores - Parte 2

Mapa Mental

Protocolos de Comunicação

MODELO OSI	PROTOCOLOS	UNIDADE DE DADOS	DISPOSITIVOS ASSOCIADOS	ARQUITETURA TCP/IP
APLICAÇÃO FORNECE INTERFACE COM O USUÁRIO E POSSIBILITA O ACESSO A RECURSOS DE REDE.	HTTP, HTTPS, FTP, SSH, TELNET, IRC, SNMP, POP3, IMAP, DNS.	DADOS		APLICAÇÃO
APRESENTAÇÃO FUNCIONA COMO UM TRADUTOR; CONVERTE CARACTERES EM CÓDIGOS; CRIPTOGRAFA E COMPRIME DADOS, ETC.	SSL, TLS, XDR.	DADOS		
SESSÃO CONTROLA O DIÁLOGO DE REDE; ESTABELECE, GERENCIA E ENCERRA SESSÕES (CONEXÕES).	NETBIOS	DADOS		
TRANSPORTE ORGANIZA OS DADOS EM SEGMENTOS E GARANTE QUE CHEGUEM AO DESTINO LIVRES DE ERROS (FORNECE CONEXÃO FIM-A-FIM.	TCP, UDP, NETBEUI.	SEGMENTOS		TRANSPORTE
REDE RESPONSÁVEL PELO ENCAPSULAMENTO DOS DADOS EM PACOTES; E PELO ENDEREÇAMENTO, ROTEAMENTO E ENTREGA DELES.	IP, ICMP, ARP, RARP, NAT.	PACOTES	ROTEADOR	INTERNET
ENLACE ORGANIZA BITS EM FRAMES E FORNECE ENTREGA NÓ A NÓ.	ETHERNET, TOKEN RING, BLUETOOTH, WI-FI	FRAMES/ QUADROS	BRIDGE SWITCH ACCESS POINT PLACA DE REDE	ENLACE / ACESSO A REDE
FÍSICA RESPONSÁVEL POR TRANSMITIR BITS ATRAVÉS DE UM MEIO FÍSICO; PROVÊ ESPECIFICAÇÕES MECÂNICAS E ELÉTRICAS.	USB, DSL.	BITS	HUB	

@mapasdathai

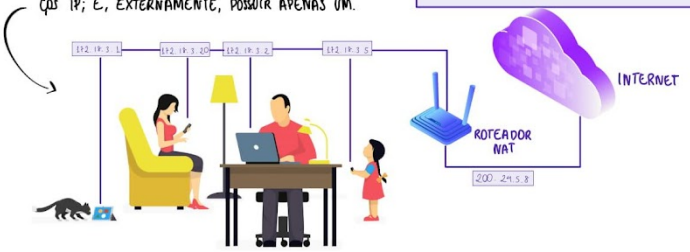
Protocolos da Camada de Rede

IP (Internet Protocol)

- PROTOCOLO PARA COMUNICAÇÃO ENTRE REDES.
- É O PROTOCOLO DE DISTRIBUIÇÃO DE PACOTES NÃO CONFIÁVEL, DE MELHOR ESFORÇO E SEM CONEXÃO, QUE FORMA A BASE DA INTERNET.
- O ENDEREÇO IP DEFINE DE FORMA ÚNICA E UNIVERSAL A CONEXÃO DE UM DISPOSITIVO.

- IP ESTÁTICO/FIXO: NÃO MUDA. É POUCO USADO E MAIS COMUM EM MÁQUINAS SERVIDORAS.
- IP DINÂMICO: MUDA A CADA CONEXÃO. É USADO EM REDES DOMÉSTICAS.

- NETWORK ADDRESS TRANSLATION (NAT): PERMITE A UM USUÁRIO TER INTERNAMENTE, EM SUA REDE DOMÉSTICA, UMA GRANDE QUANTIDADE DE ENDEREÇOS IP; E, EXTERNAMENTE, POSSUIR APENAS UM.



IPV4 (IP VERSÃO 4)	IPV6 (IP VERSÃO 6)
• POSSUI 32 BITS;	• POSSUI 128 BITS;
• REPRESENTAÇÃO DECIMAL;	• REPRESENTAÇÃO HEXADECIMAL;
• 4 BLOCOS DE 8 BITS;	• 8 GRUPOS DE 16 BITS;
• SEPARADOS POR PONTO (.).	• SEPARADOS POR DOIS-PONTOS (:).

ICMP (Internet Control Message Protocol)

- É UM PROTOCOLO AUXILIAR AO PROTOCOLO IP.
- COMUNICA OCORRÊNCIA DE SITUAÇÕES ANORMAIS NA TRANSFERÊNCIA DE PACOTES.
  - ↳ O PROTOCOLO IP NÃO POSSUI MECANISMOS INTEGRADOS PARA CONTROLE E NOTIFICAÇÃO DE ERROS.

ARP (Address Resolution Protocol)

- RESPONSÁVEL POR MANTER UMA TABELA DE CONVERSÃO DE ENDEREÇOS LÓGICOS EM ENDEREÇOS FÍSICOS.
  - ↳ ENDEREÇO IP
  - ↳ ENDEREÇO MAC
- RARP (REVERSE ARP) → RESPONSÁVEL POR FAZER O SENTIDO CONTRÁRIO.
  - ↳ MAPEIA ENDEREÇOS MAC PARA ENDEREÇOS IP.

@mapasdathai

Protocolos da Camada de Transporte

TCP (Transmission Control Protocol)

- É ORIENTADO A CONEXÕES.
  - ↳ PORQUE COMUNICA O DESTINATÁRIO QUE ENVIARÁ PACOTES ANTES DE ENVIÁ-LOS DE FATO.
- É CONFIÁVEL.
  - ↳ É CAPAZ DE ESTABELECER UMA CONEXÃO INICIAL, DE RECUPERAR PACOTES PERDIDOS, ELIMINAR PACOTES DUPLICADOS, RECUPERAR DADOS CORROMPIDOS, ETC.
- IMPLEMENTA CONTROLE DE CONGESTIONAMENTO.
- IMPLEMENTA CONTROLE DE FLUXO.
- PERMITE CONEXÃO FIM-A-FIM.
  - ↳ IGNORA QUAISQUER NÓS INTERMEDIÁRIOS QUE EXISTAM ENTRE EMISSOR E DESTINATÁRIO.
- MONITORA, ACOMPANHA, RASTREIA, CONTROLA E GERENCIA TODO O TRANSPORTE DA INFORMAÇÃO.
  - ↳ ASSIM GARANTE QUE TODOS OS PACOTES CHEGARÃO ÍNTEGROS, EM TEMPO E NA ORDEM CORRETA.

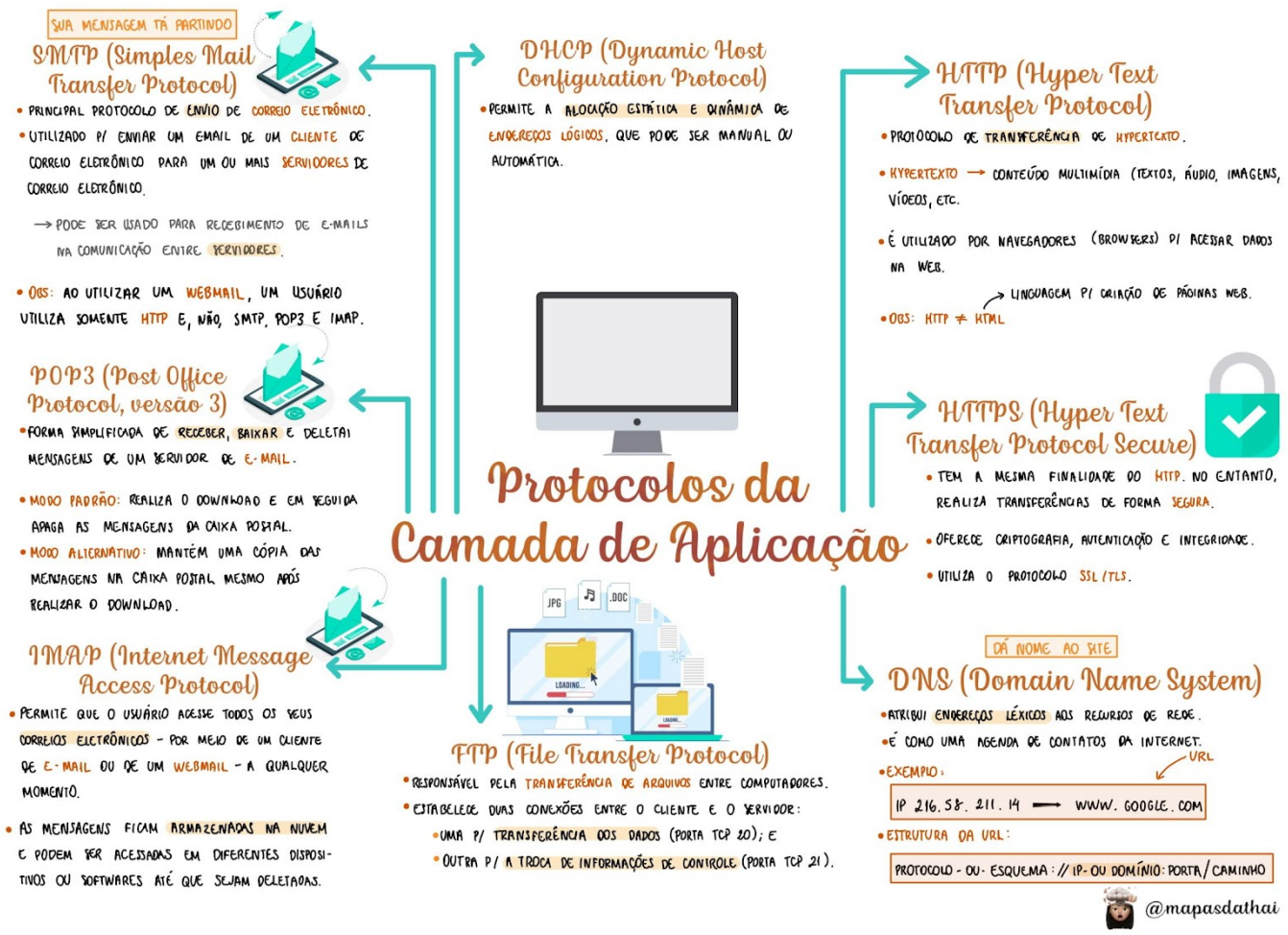
Principais portas

PROTOCOLO (CAMADA DE APLICAÇÃO)	PROTOCOLO (CAMADA DE TRANSPORTE)	Nº DA PORTA
HTTP	TCP	80
HTTPS	TCP	443
POP3	TCP	110
SMTP	TCP	25/587
IMAP3	TCP	220
IMAP4	TCP	143
FTP	TCP	20/21
TELNET	TCP	23
SSH	TCP	22
DNS	TCP/UDP	53
DHCP	UDP	67/68
IRC	TCP	194
SNMP	UDP	161/162

UDP (User Datagram Protocol)

- FORNECE SERVIÇO DE ENTREGA SEM CONEXÃO E NÃO CONFIÁVEL.
  - ↳ SEM CONTROLE DE FLUXO E DE ERROS.
- POSSUI BAIXO OVERHEAD (TRÁFEGO ADICIONAL DESNECESSÁRIO).

@mapasdathai



Questões Comentadas - Redes de Computadores - Parte 2 - MULTIBANCAS

#VamosPraticar#

14.(CS-UFG / UFG – 2017)

Um funcionário está acessando o site de um dos fornecedores da empresa, no endereço http://fornecedor.org/ [56]. Em um determinado momento, o site apresenta um formulário solicitando diversas informações. Antes de preencher o formulário, o funcionário quer saber se o site é seguro, no sentido de ter as informações transmitidas por meio de uma conexão criptografada.

Qual endereço indica que o site é seguro?

a) http://siteseguro.org/fornecedor.org/formulario/ [57]

b) sec://firewall/fornecedor.org/formulario/

c) https://fornecedor.org/formulario/ [58]

d) http://https.fornecedor.org/formulario/ [59]

Comentários:

O protocolo da camada de aplicação (HTTPS) tem a mesma finalidade do HTTP. Ele é responsável pela transferência, formatação e apresentação de páginas web com conteúdo multimídia (textos, áudio, imagens, etc) entre um servidor e um cliente. No entanto, ele realiza transferências de forma segura e criptografada, oferecendo autenticação e integridade às páginas de um Servidor Web.

Gabarito: Letra C

#VamosPraticar#

#VamosPraticar#

27.(ITAME / Prefeitura de Aragoiânia – 2016)

Assinale a alternativa correta:

a) POP3 é um protocolo de envio de e-mails.

b) FTP é um protocolo utilizado para transferência de arquivos.

c) SMTP é um protocolo de recebimento de emails.

d) HTTPS é um protocolo criado somente para trafegar voz na internet.

Comentários:

(a) Errado. POP3 é um protocolo de recebimento de e-mails; (b) Correto. FTP é realmente um protocolo utilizado para transferência de arquivos; (c) Errado. SMTP é um protocolo de envio de e-mails; (d) Errado. HTTPS é um protocolo seguro para transferência de hipertexto.

Gabarito: Letra B

#VamosPraticar#

#VamosPraticar#

37.(SELECON / Prefeitura de Cuiabá/MT – 2015)

Um internauta baixou o arquivo ccleaner-5-38- 6357.exe do site do fabricante na internet para viabilizar a instalação do software Ccleaner em seu computador. O procedimento de baixar um arquivo da internet para o computador de um usuário é conhecido pelo seguinte termo**:**

a) download

b) downsize

c) upload

d) upsize

Comentários:

O procedimento de baixar um arquivo da internet para o computador de um usuário é conhecido pelo termo: download.

Gabarito: Letra A

#VamosPraticar#

#VamosPraticar#

43.(CEPERJ / FSC – 2014)

Atualmente, é comum baixar softwares de sites da internet como as atualizações de antivírus e, paralelamente, enviar arquivos para sites de hospedagem web. Essas atividades são conhecidas, respectivamente, por:

a) download e upload

b) upload e download

c) download e downlink

d) downlink e uplink

e) uplink e downlink

Comentários:

Baixar softwares de sites da internet é um exemplo de download; enviar arquivos para sites de hospedagem web é um exemplo de upload.

Gabarito: Letra A

#VamosPraticar#

Referências e links deste capítulo

1 http://www.whatismyip.com

2 http://www.estrategiaconcursos.com.br

3 http://www.estrategiaconcursos.com.br:80

4 http://www.estrategiaconcursos.com.br:80

5 http://www.estrategiaconcursos.com.br:80

6 http://www.estrategiaconcursos.com.br:21

7 http://www.estrategiaconcursos.com.br:21

8 http://www.estrategiaconcursos.com.br:21

9 mailto:diego@gmail.com

10 mailto:renato@gmail.com

11 http://gmail.com

12 mailto:diego@gmail.com

13 mailto:renato@yahoo.com

14 mailto:renato@yahoo.com

15 mailto:renato@yahoo.com

16 mailto:renato@yahoo.com

17 mailto:renato@yahoo.com